



HP StorageWorks Reference Information Storage System Administrator Guide

Product Version: 1.1

First Edition (February 2005)

Part Number: T3559-96001

© Copyright 2004-2005 Hewlett-Packard Development Company, L.P.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information contained in this document is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Microsoft® and Windows® are US registered trademarks of Microsoft Corporation.
Outlook™ is a trademark of Microsoft Corporation.

Parts of this guide are copyrighted by SHERPA SOFTWARE GROUP, L.P. All rights reserved.

HP StorageWorks Reference Information Storage System Administrator Guide
First Edition (February 2005)
Part Number: T3559-96001

Contents

Chapter 1: RISS overview

RISS	1-2
RIM	1-3

Chapter 2: Platform Control Center

Tour of PCC user interface	2-3
Accessing PCC	2-3
User interface components	2-3
User interface orientation tips	2-4
Views for common tasks	2-6
Updating views before printing	2-7
Printing view frames	2-7
Left menu views	2-8
Monitoring and reporting tool	2-11
Monitoring and reporting methods	2-11
Statuses and states	2-12
Status Summary view	2-17
Checking system health	2-18
Displaying hosts with a specific status	2-18
Displaying services with a specific status	2-19
Displaying specific host groups	2-19
Displaying specific host groups and host statuses	2-19
Displaying specific host groups and service statuses	2-19
System Status view	2-20
Displaying software versions	2-23
Displaying the Smart Cell Groups for Domain view	2-23
Application Management view	2-25
Starting, stopping, and restarting servers on the system	2-27
User Management view (Dynamic Account Synchronization)	2-28
Configuring DAS	2-28
Updating connections to LDAP servers	2-33
Deleting connections to LDAP servers	2-33

Displaying DAS configuration associations	2-33
Deleting DAS configuration associations	2-33
Updating or deleting mappings	2-33
Updating or deleting assignments	2-34
Starting or scheduling DAS jobs	2-34
Displaying servers with assigned DAS configurations	2-35
Smartcell Cloning view	2-36
Cloning smart cells (copying data)	2-38
Replication view	2-39
Displaying replication statuses for groups in a domain and replication performance over time	2-40
Starting replication for specific domains	2-41
Stopping replication for specific domains	2-41
Selective Archiving folder	2-42
Mining Overview view	2-42
Miner 1	2-45
System Backup view	2-46
Monitoring folder	2-50
Tactical Monitoring view	2-50
Service Detail view	2-53
Host Detail view	2-56
Service Overview view	2-58
Service Problems view	2-61
Host Problems view	2-62
Comments view	2-63
Host Downtime view	2-65
Nagios folder	2-68
Nagios Info view	2-68
Nagios Stats view	2-71
Scheduling Queue view	2-73
Reporting folder	2-75
Email Reporter view	2-75
LogFile Sender view	2-81
Trends view	2-81
Availability view	2-85
Notifications view	2-89
Event Log view	2-92

Alerts folder	2-94
Alerts Histogram view	2-94
Alerts History view	2-97
Alerts Summary view	2-100
Software Version view	2-106
Viewing software versions on the system	2-106
Displaying the patch history	2-106
View Config view	2-107
Services tools folder	2-113
View Cell Space view	2-113
Restoring data on failed smart cells	2-116
MBean view	2-117
Agent view	2-118
Warnings folder	2-120
All Warnings view	2-120
Additional views	2-121
Hostgroup Information view	2-121
Host Information view	2-126
Host Commands section	2-128
Adding comments for specific hosts	2-131
Deleting all comments for specific hosts	2-132
Service Information view	2-133
Service Commands section	2-135
Adding comments for specific services	2-139
Deleting all comments for specific services	2-140
Status Grid view	2-141
Displaying specific hostgroups	2-142
Displaying specific hosts	2-142
Displaying all services running on specific hosts	2-142
Displaying specific services	2-142
External Command Interface view	2-143

Chapter 3: Platform Account Manager

PAM overview	3-2
User accounts	3-2
Installing PAM	3-2
Logging in to PAM	3-3
PAM window	3-4

Performing basic PAM tasks	3-8
Creating PAM objects	3-8
Viewing PAM objects	3-8
Modifying PAM objects	3-10
Deleting PAM objects	3-11
Adding member objects to collection objects	3-12
Removing member objects from collection objects	3-13
Managing user accounts	3-14
Accessing Users panel	3-14
Filtering list of users	3-16
Viewing non-editable user information	3-16
Adding new users	3-17
Modifying email information	3-17
Viewing and modifying user comments	3-18
Managing repositories	3-19
Accessing Repositories panel	3-19
Filtering list of repositories	3-20
Viewing non-editable repository information	3-21
Adding repositories	3-21
Adding ACLs to repositories	3-22
Removing ACLs from repositories	3-22
Managing access control lists (ACLs)	3-23
Accessing ACLs panel	3-23
Filtering list of ACLs	3-24
Viewing non-editable ACL information	3-24
Adding ACLs	3-25
Adding users to ACLs	3-25
Removing users from ACLs	3-25
Viewing user profiles	3-26
Managing routing rules	3-27
Accessing Routing Rules panel	3-27
Filtering list of routing rules	3-28
Viewing non-editable routing rule information	3-28
Adding routing rules	3-29
Modifying routing rules	3-30
Deleting routing rules	3-30
Adding repositories to routing rules	3-30
Managing simple routing rules	3-31
Accessing Simple Routing Rules panel	3-31
Filtering list of simple routing rules	3-32

Viewing non-editable simple routing rule information	3-32
Adding simple routing rules	3-33
Adding repositories to simple routing rules	3-33
Removing repositories from simple routing rules	3-33
Managing routing filters	3-34
R0000000 Catchall Repository	3-34
Routing filter examples	3-35
Accessing Routing Filters panel	3-36
Filtering list of routing rules	3-37
Adding routing filters	3-37
Modifying routing filters	3-38
Deleting routing filters	3-38
Example: Integrating new department	3-39
Problem statement and solution	3-39
Creating marketing department users	3-41
Creating ACL for managers to access marketing email	3-42
Creating repository for marketing department	3-42
Editing simple routing rules for marketing email	3-43

Chapter 4: PST Importer

PST Importer overview	4-2
PST Importer process	4-2
Archive Request file	4-3
Installing PST Importer	4-4
Installation requirements	4-4
Installation procedure	4-5
Using PST Importer	4-6
Archive Request Loader	4-6
PST Import Monitor	4-11
Archive Request file	4-16
Settings description	4-16
Sample file	4-19

Chapter 5: Configuring Outlook or Lotus Notes

Configuring your system for Exchange and Outlook	5-2
Configuring user accounts on customer servers	5-2
Configuring Journal Mining	5-3
Configuring Mailbox Mining	5-5
Configuring non-sticky ports	5-7

Installing the Outlook plug-in	5-8
Configuring your system for Lotus Domino and Lotus Notes	5-14
Requirements for Domino server configuration	5-14
Installing Email Miner for Lotus Notes	5-15
Administering Email Miner for Lotus Notes	5-15
Installing and configuring the Lotus Notes plug-in	5-15

Appendix A: Email Miner Version P2.0 for Lotus Notes Installation Guide

Overview	A-2
Architecture	A-2
Frequently asked questions	A-2
System requirements and prerequisites	A-5
Available platforms and restrictions	A-6
Email Miner	A-7
Installation	A-7
Error messages	A-12

Appendix B: Email Miner Version P2.0 for Lotus Notes Administration Guide

Email Miner	B-2
Overview	B-2
Security	B-2
Mail server configuration	B-3
Mail user configuration	B-9
Selective archiving	B-13
Agents	B-19
Error messages	B-20
Dialog Box messages	B-20
Email notifications	B-21
Log messages	B-21

CHAPTER 1

RISS overview

This chapter describes key concepts involving the HP StorageWorks Reference Information Storage System (RISS) and Reference Information Manager (RIM).

This chapter contains these topics:

- [RISS, on page 1-2](#)
- [RIM, on page 1-3](#)

RISS

The Reference Information Storage System (RISS) is a fault-tolerant, secure system of hardware and software that archives files and email messages for your organization, and lets you search for archived documents. RISS provides the following main functions:

- Automatic, active **data archiving** (email and specific document types) that helps your organization meet regulatory requirements.
- Interactive **data querying** to search for and retrieve archived data according to various criteria.

See also

- *HP StorageWorks Reference Information Storage System User Guide*, for information about querying data
- [Chapter 2, Platform Control Center](#)
- [Chapter 3, Platform Account Manager](#)

RIM

Reference Information Manager (RIM) is management software supplied with RISS. To interact with the system, users can access the following applications:

Table 1-1: RIM applications for users

Application	Tasks
RISS Web Interface	Use a web browser to search for documents archived on the system. Save and reuse search-query definitions and results.
RISS Outlook Interface (customer option)	Search for emails using Microsoft Outlook with a Microsoft Exchange mail server. View and work with archived emails.
RISS Lotus Notes Interface (customer option)	Search for emails using IBM Lotus Notes with an IBM Domino mail server. View and work with archived emails.
Document Manager (customer option)	Manually archive files by placing copies in a special Windows folder.

RIM provides the following troubleshooting and administrative tools:

Table 1-2: RIM applications for administrators

Application	Tasks
PCC (Platform Control Center)	Monitor and troubleshoot system status and performance. See Chapter 2, Platform Control Center .
PAM (Platform Account Manager)	Manage user accounts. See Chapter 3, Platform Account Manager .

Table 1-2: RIM applications for administrators

Application	Tasks
PST Importer	Use for batch processing of multiple PST files. See Chapter 4, <i>PST Importer</i> .
Mail Attender for Exchange	Create selective archiving rules for Microsoft Exchange and Outlook. See Configuring your system for Exchange and Outlook , on page 5-2.
Email Miner	Create selective archiving rules for IBM Domino and Lotus Notes. See Configuring your system for Lotus Domino and Lotus Notes , on page 5-14.

CHAPTER 2

Platform Control Center

This chapter describes the Platform Control Center (PCC) tool for monitoring and troubleshooting RISS.

It includes these topics:

- [Tour of PCC user interface, on page 2-3](#)
- [Status Summary view, on page 2-17](#)
- [System Status view, on page 2-20](#)
- [Application Management view, on page 2-25](#)
- [User Management view \(Dynamic Account Synchronization\), on page 2-28](#)
- [Smartcell Cloning view, on page 2-36](#)
- [Replication view, on page 2-39](#)
- [Selective Archiving folder, on page 2-42](#)
- [System Backup view, on page 2-46](#)
- [Monitoring folder, on page 2-50](#)
- [Nagios folder, on page 2-68](#)
- [Reporting folder, on page 2-75](#)
- [Alerts folder, on page 2-94](#)
- [Software Version view, on page 2-106](#)
- [View Config view, on page 2-107](#)
- [Services tools folder, on page 2-113](#)

- [Warnings folder, on page 2-120](#)
- [Additional views, on page 2-121](#)

Tour of PCC user interface

Accessing PCC

To access PCC, open a web browser, and type the RISS server's administrative IP address.

User interface components

PCC is an HTML-based application containing a menu on the left side of the page (referred to as the **left menu**). Use the left menu to access most views in PCC.

All PCC views contain the left menu. Some views also contain a gray box heading, links to related views, and a help button.

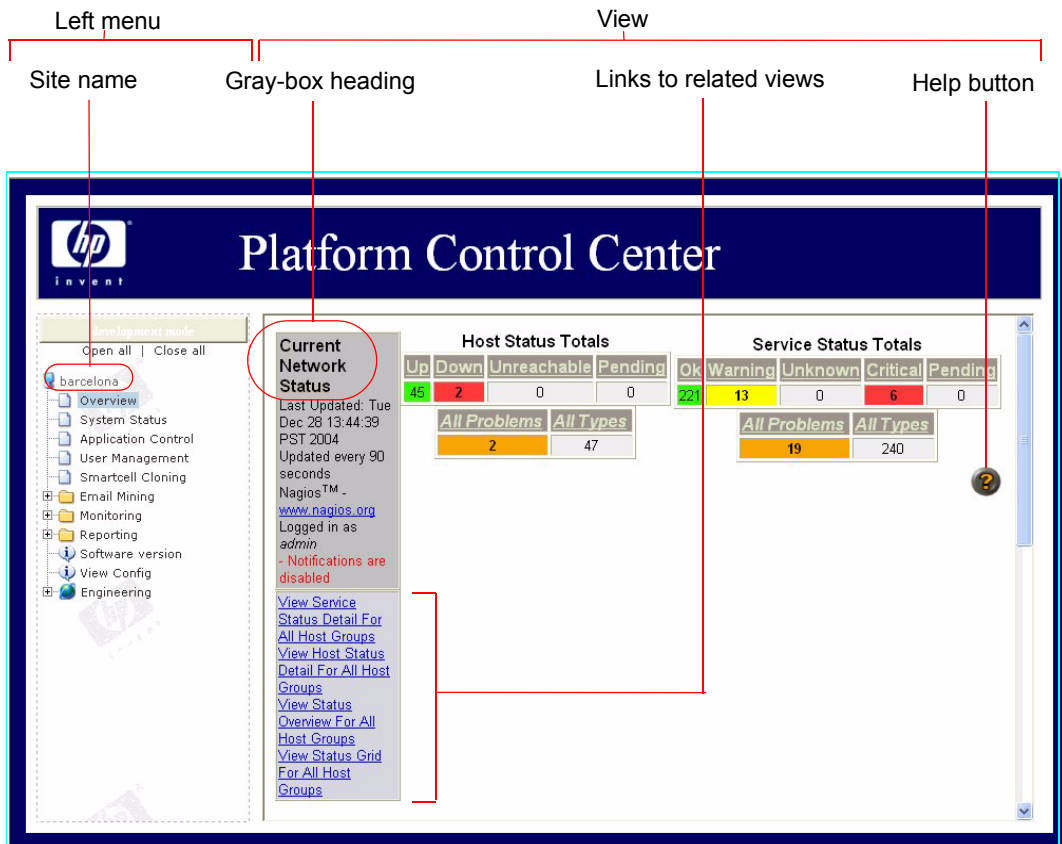


Figure 2-1: Platform Control Center user interface

User interface orientation tips

Views are often associated with several names or brief descriptions. To orient yourself, pay attention to the different ways a view is characterized.

- *Link text:* A navigation link leading to a view is often the most specific description of the view.

For example, the link View Status Detail For This Host displays the Host Detail view for a specific host; the link View Host Status Detail For All Hosts displays the Host Detail view for all hosts.

- *Gray-box heading:* Some views have a gray box in the upper-left corner containing information about the latest view update and update

frequency (see [User interface components, on page 2-3](#), for an illustration). The heading sometimes provides an additional characterization of the view.

For example, the gray-box heading for the Nagios Stats view is Performance Information, indicating the view displays performance information about the Nagios monitoring process.

- *Filter description:* Information that is a subset of information obtained by filtering another view is sometimes indicated by a gray box entitled Display Filters. The box describes filtering used.

For example, the Service Problems view provides a subset of information in the Service Detail view. The Display Filters box indicates Service Status Types shown are All Problems.

- *Chart heading:* Some views have several charts. The heading of the most prominent chart often reflects the main purpose of the view (see [User interface components, on page 2-3](#), for an illustration).

For example, when the Service Detail view shows information about a single host, the most prominent chart in the view is entitled Service Status Details For Host *<hostname>*.

- *HTML name:* Each PCC view has a descriptive HTML name. A view normally appears in the browser as an HTML frame alongside the left menu, which is another frame. You usually see a view's HTML name when you:
 - Print only the view, not the view and left menu. Depending on the browser and its configuration, the HTML name can appear in printed page headers.

For example, if you print the frame of the Event Log view, the printed page header may be Nagios Log File.
 - Open the view address (URL) in a browser window by itself, without any frames (without left menu). The browser window title shows the view's HTML name.

For example, if you open the link Event Log in a separate window, the window title is Nagios Log File.

See Also

- [Updating views before printing, on page 2-7](#)

- [Printing view frames, on page 2-7](#)

Views for common tasks

Table 2-1: Views for common system administration tasks

Task	View
Check system health	Status Summary view, on page 2-17 If everything is green, system is healthy. If something is red, click on it to zoom in and examine the problem.
Check system performance	Status Summary view, on page 2-17 High store and indexing rates are good. Low query times are good. To zoom in on an hourly period, click the period in the Last 24 Hours bar.
Check smart cell health and performance	Displaying the Smart Cell Groups for Domain view, on page 2-23
Check backup status	System Backup view, on page 2-46
Clone smart cells (copy data)	Smartcell Cloning view, on page 2-36
Monitor system alerts	Alerts History view, on page 2-97
Configure periodic email reports of system status and performance	Email Reporter view, on page 2-75
Enable automatic email notifications for important system events, such as host or service problems and recoveries	Nagios Info view, on page 2-68
Communicate problems, instructions, and so on as comments; and read co-workers' comments	Comments view, on page 2-63
Start, stop, and restart servers on the system	Application Management view, on page 2-25
Monitor, start, and stop replication for domains	Replication view, on page 2-39

Table 2-1: Views for common system administration tasks (continued)

Task	View
Display status information about email mining servers	Mining Overview view, on page 2-42

Updating views before printing

PCC views displayed in the web browser are automatically updated approximately every 90 seconds. To manually update the view, click Refresh (or Reload) in the browser.

If the browser caches web pages, the cached view displayed when you click the browser's Back button can be out of date. Refresh it manually.

Some browsers print from an updated version of the web page without refreshing the browser display. If the displayed view is out of date, the printout can appear different from the displayed view. To ensure you print what is displayed, refresh the browser manually before printing.

Printing view frames

The PCC web browser interface is an HTML (web) page composed of two HTML frames. The left frame contains the left menu. The right frame contains the current view. To print the current view, print the view frame, not the left menu frame or entire page (both frames). See the browser's documentation for instructions on printing frames.

Left menu views

The left menu provides quick access to many PCC views. Shaded cells in Table 2-2 indicate the most commonly used views.

Table 2-2: Views accessible from left menu

Left menu item	Description	Page
Status Summary view	View high-level summary of system health. For each host group, shows how many hosts and services have each status value. View status of each host group without details.	2-17
System Status view	View summary of system domains, smart cells, exceptions, and current software versions. View system performance graphs. View summary of system capacity and performance.	2-20
Application Management view	Start, stop, or restart one or more servers on the system.	2-25
User Management view (Dynamic Account Synchronization)	Configure Dynamic Account Synchronization to automatically create and update RISS users with information obtained from LDAP servers.	2-28
Smartcell Cloning view	Clone smart cells (copy data) to give them a new, viable mirror cell.	2-36
Replication view (Optional)	Monitor and start or stop replication for domains.	2-39
Mining Overview view	View status of mining system on each domain. View graphs of message store rate.	2-42
Miner 1	Provides VNC access to the email miner.	2-45
System Backup view (Optional)	View state and status information about backup server and services, including which backup services are enabled, results of last backup, and alerts or warnings.	2-46

Table 2-2: Views accessible from left menu (continued)

Left menu item	Description	Page
Tactical Monitoring view	View high-level summary of system health and monitoring, showing how many hosts and services have each status value and which monitoring features are enabled. Set monitoring features.	2-50
Service Detail view	View status of services running on each host, organized by host groups. Examine details of particular services.	2-53
Host Detail view	View status information for each host in the system. Examine details of particular hosts.	2-56
Service Overview view	View status of hosts in each host group. View high-level summary of status of services on each host.	2-58
Service Problems view	View status information for each service that has a problem (subset of Service Detail view). Examine details of problem services.	2-61
Host Problems view	View status information for each host that has a problem (subset of Host Detail view). Examine details of problem hosts.	2-62
Comments view	View system administrators' comments. Add comments to communicate with other system administrators.	2-63
Host Downtime view	View scheduled host and service downtimes. Schedule host and service downtimes, disabling notifications during downtimes.	2-65
Nagios Info view	View information about PCC host and service monitor. Control monitoring, check monitoring status, and enable and disable notifications globally for all hosts and services.	2-68
Nagios Stats view	View information about performance of PCC host and service monitoring. Check monitoring performance.	2-71

Table 2-2: Views accessible from left menu (continued)

Left menu item	Description	Page
Scheduling Queue view	View scheduled service checks for each host in the system. Schedule service checks.	2-73
Email Reporter view	Configure summary monitoring reports to be sent periodically to email recipients you choose.	2-75
LogFile Sender view	Select log files to send to HP to assist in troubleshooting.	2-81
Trends view	Create status reports for individual hosts or services over given time periods.	2-81
Availability view	Create availability reports for individual hosts, services, or host groups over given time periods.	2-85
Alerts Histogram view	Create reports with simple graphs for different time periods. For individual hosts or services, shows number of events for each status value.	2-94
Alerts History view	View most recently logged alerts.	2-97
Alerts Summary view	Create reports summarizing different types of alerts over different periods.	2-100
Notifications view	View host and service notifications sent to system contact (admin).	2-89
Event Log view	View most recently logged events.	2-92
Software Version view	View software versions of hosts in the system.	2-106
View Config view	View summaries of entire system configuration from various viewpoints based on object types (such as hosts, services, contacts, and commands). Examine system parameters defined during system configuration.	2-107
View Cell Space view	View names of important hosts organized by host groups. View life cycle states and health of smart cells in each domain. Determine status of data archiving system.	2-113

Table 2-2: Views accessible from left menu (continued)

Left menu item	Description	Page
All Warnings view	View exceptions (warnings) for the system.	2-120

See Also

- [User interface components, on page 2-3](#), for more information about the left menu
- [Displaying the Smart Cell Groups for Domain view, on page 2-23](#), for information about a commonly used view that is inaccessible from the left menu

Monitoring and reporting tool

PCC monitors the system and reports on its health and activity. PCC provides reports on:

- system health (status)
- system performance
- smart cell states

Hosts in the system (and their services) are organized into groups of the same type, called **host groups**. For example, to look at all hosts of type smart cell, display the status of the host group Smart Cells.

PCC refers to the behind-the-scenes monitoring functions and the user interface reporting the findings. In both roles, the system uses software provided by Nagios, www.nagios.org. (PCC is part of the system it monitors, so it monitors itself, as well. See [Nagios Info view, on page 2-68](#), and [Nagios Stats view, on page 2-71](#).)

Monitoring and reporting methods

System monitoring is reported online with a web-based (HTML) user interface and offline by email to selected contacts. Email reporting provides a subset of information provided online.

Hosts and services are monitored by polling. You schedule polling intervals for services, but host polling is purposely kept to a minimum. Depending on the polling interval, there is more or less delay between occurrences on the system and reporting those occurrences in the PCC interface. In general, a host is polled only at system startup and after one or more service checks indicate a potential host problem. As long as services appear to be functioning correctly (OK), the host is assumed to be healthy (UP). You can selectively enable or disable hosts and services polling.

If monitoring indicates a host is not functioning correctly (DOWN), none of its services are available (they can have any status except OK). If a service has CRITICAL status, but the host is UP, the service probably needs to be restarted.

See Also

- [Host and service status values, on page 2-14](#)

Statuses and states

Various PCC views show current life cycle **states** of smart cells or **status values** of particular hosts or services. Status values measure relative health, and can be associated with a **status condition** conveying a measure of confidence in the reported value. This section defines possible life cycle states, status values, and status conditions.

For example, the health of a smart cell in the life cycle state DEAD can be reported with the host status value DOWN. If the host status value has been checked the required number of times, the status condition is reported as HARD (otherwise, it is SOFT).

PCC views (see [User interface components, on page 2-3](#)) often use “status” and “state” loosely and interchangeably when referring to hosts and services. “State” is always used when referring to smart cell life cycle states, but “status” and “state” are both used when reporting smart cell health, regarding it as a host like any other. PCC views also refer to status conditions as “states” or “state types.”

System component status is color coded: **green** indicates normal operation; **red** indicates component has stopped or failed; **yellow** indicates a warning. See [Host and service status values, on page 2-14](#).

Smart cell life cycle states

Table 2-3: Smart cell life cycle states

Life cycle state	Definition	Importance
DISCOVERY	Metaserver and smart cell are determining cell's start state (state following DISCOVERY), based on expected states of the cell and its mirror smart cell. Cell is not available for document storage, search, or retrieval.	maintenance (startup only)
ASSIGNED	Cell is assigned to a domain. Cell is available for document storage, search, and retrieval. If backup is enabled, cell data can be backed up.	normal
COMPLETE_PROCESSING	Data indexing is being completed. Cell is full. Cell is available for document search and retrieval, but not storage. If backup is enabled, cell data can be backed up.	maintenance
BACKING_UP	Cell is available for document search and retrieval. If backup is enabled, cell is backing up all its indexes and new data that has not yet been backed up.	maintenance
SYNC_WAIT	Cell is available for document search and retrieval.	maintenance
CLOSED	Cell is full. Cell is available for document search and retrieval, but not storage. If backup is enabled, all cell data was backed up before cell entered this state.	normal
RESET	Cell is being recycled. Stored documents and corresponding management data, such as document indexes, are destroyed during recycling. System administrator determined existing cell data is no longer needed. The RESET state is only set manually. Cell is not affiliated with any domain, so it is not available for document storage, search, or retrieval.	maintenance
FREE	Cell can become ASSIGNED or become a target for data restoration. Cell is not affiliated with any domain, so it is not available for document storage, search, or retrieval.	normal

Table 2-3: Smart cell life cycle states (continued)

Life cycle state	Definition	Importance
RESTORE	Cell is a target for data restoration from another smart cell. Cell is not available for document storage, search, or retrieval.	maintenance
DEAD	Cell requires attention. Cell is not available for document storage, search, or retrieval. If backup is enabled, some or all cell data might <i>not</i> be backed up; if so, data will <i>never</i> be backed up.	failure
SUSPENDED	Either of the following is true: <ul style="list-style-type: none"> Cell or its mirror cell has one or more failed processes. In this case, both are SUSPENDED. Mirror cell is DEAD. <i>Note:</i> If the cell's Application Health service is OK, only the mirror cell failed. (Use the Service Detail view to check this service.) Cell is not available for storage. Cell is available for document search and retrieval (unless a failed process disabled the search engine). If backup is enabled, cell is backing up new data that has not yet been backed up.	failure

Host and service status values

Shading in Table 2-4 and Table 2-5 indicates normal values.

Table 2-4: Host status values

Status	Color	Description
PENDING	Gray	Host has not yet been checked for status. When PCC starts monitoring services associated with a host, the host status value is set to PENDING.
UP	Green	Host is running, and responds to status checks.
DOWN	Red	Host is not running, and does not respond to status checks.

Table 2-4: Host status values (continued)

Status	Color	Description
UNREACHABLE	Brown	Parent cloud router of the UNREACHABLE smart cell or HTTP portal is DOWN.

Table 2-5: Service status values

Status		Description
PENDING	Gray	Service has not been checked for status since PCC monitoring started.
OK	Green	Service is functioning normally.
WARNING	Yellow	Service might have a problem.
UNKNOWN	Orange	Service status cannot be determined.
CRITICAL	Red	Service is not functioning correctly. Data storage and/or search and retrieval are adversely affected.

See Also

- [Hard and soft status conditions, on page 2-15](#), for information about relative confidence of host and service status values.
- [Monitoring and reporting tool, on page 2-11](#), for information about determining status values.

Hard and soft status conditions

Host or service status values are reported in alerts and other events as having a HARD or SOFT status condition (also referred to in monitoring views as “state type”). See, for example, the following views:

- [Alerts Histogram view, on page 2-94](#)
- [Alerts History view, on page 2-97](#)
- [Alerts Summary view, on page 2-100](#)
- [Event Log view, on page 2-92](#)

A SOFT status condition indicates the status value has not yet been confirmed; a HARD status condition has been confirmed. Confirmation is required only for problem status values, not for normal operation values (UP for hosts, OK for services). A normal status value always has a HARD status condition.

When host or service problems are detected, PCC rechecks the problem a certain number of times. During this trial period, the status condition is considered SOFT. After rechecking the required number of times with the same result, the status condition is considered HARD.

Required number of checks for a given host or service is displayed in the View Config view (Hosts or Services Object Type, respectively). See [View Config view, on page 2-107](#).

See Also

- [Host and service status values, on page 2-14](#)

Status Summary view

This view provides a high-level look at system health. Depending on how it is accessed, this view displays information about a single host group or all host groups. You can quickly see overall status of each host group.

Note: Other views use the charts Host Status Totals and Service Status Totals. These charts always refer to the set of hosts and services the view targets. For example, if a view describes a single host group, these charts show only hosts and services for that host group.

Table 2-6: Status Summary view features

Feature	Description
Host Status Totals	Number of hosts: <ul style="list-style-type: none">• with each status value (Up, Down, Unreachable, Pending)• with a problem (Down, Unreachable, Pending)• in the system (All Types)
Service Status Totals	Number of services: <ul style="list-style-type: none">• with each service status value (Ok, Warning, Unknown, Critical, Pending)• with a problem (Warning, Unknown, Critical, Pending)• in the system (All Types)
Status Summary For . . . Host Group . . .	For each target host group, number of hosts and services with each status value.

See Also

- [Host and service status values, on page 2-14](#)

Related Views

- The Status Summary view is a subset of the Service Overview view (see [Service Overview view, on page 2-58](#)). The Status Summary view only displays number of hosts with each status value. The Service Overview view displays status value of each host. Use the Status Summary view for a concise summary of all system health.

Table 2-7: Links to Status Summary view

Origin	Link
left menu	Overview
Service Overview view, on page 2-58	View Status Summary . . .
Host Detail view, on page 2-56	View Status Summary . . .
Host Problems view, on page 2-62	View Status Summary . . .
Service Detail view, on page 2-53	View Host Status Summary . . .
Status Grid view, on page 2-141	View Status Summary . . .

Table 2-8: Links from Status Summary view

Destination	Link
Service Detail view, on page 2-53	View Service Status Detail . . .
Host Detail view, on page 2-56	View Host Status Detail . . .
Service Overview view, on page 2-58	View Service Overview . . .
Status Grid view, on page 2-141	View Status Grid . . .
Hostgroup Information view, on page 2-121	host group abbreviation, in parentheses – example: (sc)

Checking system health

In the System Status page:

- If every area is green, system is healthy.
- If any area is red, click that area to zoom in and examine the problem.

Displaying hosts with a specific status

In the System Status page, under Host Status Totals, click a status column heading, such as Down. The Service Overview view appears. See [Service Overview view, on page 2-58](#) for more information.

Displaying services with a specific status

In the System Status page, under Service Status Totals, click a status column heading, such as Critical. The Service Detail view appears. See [Service Detail view, on page 2-53](#) for more information.

Displaying specific host groups

In the System Status page, under Status Summary for HostGroup, click a Host Group name, such as Smart Cells. The Service Overview view appears. See [Service Overview view, on page 2-58](#) for more information.

In the System Status page, under Status Summary for All Host Groups, click a host group name's parenthetical abbreviation, such as (sc). The Hostgroup Information view appears. See [Hostgroup Information view, on page 2-121](#) for more information.

Displaying specific host groups and host statuses

In the System Status page, under Status Summary for All Host Groups, click the Host Status Totals column entry for a host group and status value, such as 2 DOWN. The Service Status Details view appears. See [Service Detail view, on page 2-53](#) for more information.

Displaying specific host groups and service statuses

In the System Status page, under Status Summary for All Host Groups, click the Service Status Totals column entry for a host group and status value, such as 1 CRITICAL. The Service Status Details view appears. See [Service Detail view, on page 2-53](#) for more information.

System Status view

This view provides graphical performance and resource information.

Table 2-9: System Status view features

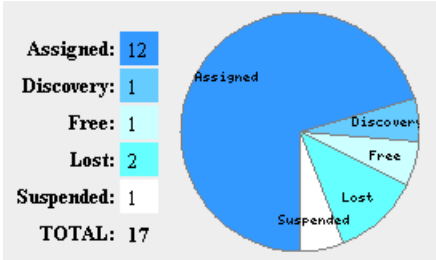
Feature	Description												
Smart Cell Domain Information	<ul style="list-style-type: none">• Name and status of domains in the system• Total number of messages currently stored in all domains• Total number of messages that could not be parsed (interpreted) or routed in all domains <p>Messages with malformed message structure (MIME) or unsupported character sets cannot be parsed. They are placed in the catch-all repository with messages that fail to be routed.</p>												
Smart Cell Allocation	<p>Number of smart cells in each life cycle state. Lost is a pseudostate indicating smart cells whose current life cycle state cannot be determined.</p> <p>Example:</p>  <p>The pie chart illustrates the distribution of smart cells across different life cycle states. The largest segment is 'Assigned' (12 cells), followed by 'Lost' (2 cells), 'Discovery' (1 cell), 'Free' (1 cell), and 'Suspended' (1 cell). The total number of smart cells is 17.</p> <table><tr><td>Assigned:</td><td>12</td></tr><tr><td>Discovery:</td><td>1</td></tr><tr><td>Free:</td><td>1</td></tr><tr><td>Lost:</td><td>2</td></tr><tr><td>Suspended:</td><td>1</td></tr><tr><td>TOTAL:</td><td>17</td></tr></table>	Assigned:	12	Discovery:	1	Free:	1	Lost:	2	Suspended:	1	TOTAL:	17
Assigned:	12												
Discovery:	1												
Free:	1												
Lost:	2												
Suspended:	1												
TOTAL:	17												
Software Versions	<p>Link displaying version identifiers for installed software groups.</p>												

Table 2-9: System Status view features (continued)

Feature	Description
Graph Information	<ul style="list-style-type: none"> • Other graphs: Link to custom performance graphs of selectable components. • 24-hour time bar: Selectable time periods for graph displayed at bottom of window. You can select Last 24 Hours or hourly periods expressed in 24-hour (military) format. Selected period has a gray background. (All times are in time zone where system is installed.) • Select box: Type of data displayed in graph at bottom of window. <ul style="list-style-type: none"> – Appliance Rates: store rate (messages stored per second), index rate (messages indexed per second), and indexer latency growth (store rate minus index rate) over selected time period. – Saved Queries: Average wait time (after query is submitted until processing starts) and completion time (after processing starts until all results are retrieved) of saved queries. – Unsaved Queries: Average wait time (after query is submitted until processing starts), first-page time (after query is submitted until first page is displayed), and completion time (after processing starts until first batch of results, 500 or less, is retrieved) of unsaved queries. • graph: Line graph showing selected performance data for selected time period. <p>In a properly operating system, indexer latency growth is zero on average over time, which means stored data is being indexed as fast as new data is being stored. Positive values mean indexing is slower than storage. Even a small positive value maintained over several days means indexing is falling further and further behind storage. Negative values generally mean indexing is catching up on backlog of documents: more stored messages are being indexed than new messages are being stored.</p> <p>To update graph, select another time period in the 24-hour time bar. For example, select 16 to display store and index rates from 16:00 to 17:00, which is 4:00 pm to 5:00 pm.</p> <p>To select another data type and update graph, click the arrow in the Select box.</p> <p>To select and view detailed graphs of system and component performance, click Other Graphs. Select component, metric, and time period. For example, you can choose to display minimum, maximum, and average performance of TSC-NAT machine from 5:00 pm to 6:00 pm on January 26, 2005.</p>

Related Views

- [Email Reporter view, on page 2-75](#), configures a periodic email report similar to the System Status view information.
- [Displaying the Smart Cell Groups for Domain view, on page 2-23](#), provides Store/Index/Indexer Latency graphs for individual smart cell groups.
- The following views report on monitoring system performance:
 - [Scheduling Queue view, on page 2-73](#)
 - [Hostgroup Information view, on page 2-121](#)
 - [Tactical Monitoring view, on page 2-50](#)

Table 2-10: Links to System Status view

Origin	Link
left menu	System Status
Displaying the Smart Cell Groups for Domain view, on page 2-23	Return to Summary
All Warnings view, on page 2-120	Return to Summary
Other Graphs view – see Other Graphs feature, System Status view features, on page 2-20	Return to Summary

Table 2-11: Links from System Status view

Destination	Link
Displaying the Smart Cell Groups for Domain view, on page 2-23	domain name (see Smart Cell Domain Information, on page 2-20)
All Warnings view, on page 2-120	host group (see All Warnings view, on page 2-120)
Other Graphs view	Other Graphs

Displaying software versions

Click Software Versions. Version identifiers for the following installed software groups appears:

- Linux Core: Third-party software on Linux servers
- Windows Core and Windows Software: Third-party software on email mining server
- Software: HP-developed Java packages
- Installer: Software on Kickstart server that installs software on other servers

Displaying the Smart Cell Groups for Domain view

This view provides performance information about each smart cell group in a domain.

Note: You typically monitor this view daily.

Table 2-12: Smart Cell Groups for Domain view features, single group

Feature	Description
smart-cell group ID number	Smart-cell group identifier generated automatically by RISS. This number is unique across all systems.
Primary	IP address of primary smart cell of group. Additional primary smart cell information:
• State	• Current life cycle state of smart cell. See Smart cell life cycle states, on page 2-13 .
• Store Rate	• Number of documents currently being stored per second.
• Index Rate	• Number of documents currently being indexed per second.
• Archived	• Number of documents archived since smart cell was assigned.
• Indexed	• Number of documents indexed since smart cell was assigned.
• Docs Failed	• Number of documents not indexed since startup.
• Last Updated	• Date and time smart cell was last updated.

Table 2-12: Smart Cell Groups for Domain view features, single group

Feature	Description
Secondary	Secondary smart cell of group. Same information as Primary (see previous).
Replica	Remote replica of one or both smart cells in group. Replicas are numbered 1 and 2. Same information as Primary (see previous).
Graph	Document storage and indexing rates, and difference between rates over last 24 hours.

See Also

- [Detailed email reports, on page 2-77](#), for information about automatically sending email reports containing the same information as the Smart Cell Groups for Domain view.

Related Views

- [System Status view, on page 2-20](#).
- Much of the information in the Smart Cell Groups for Domain view is also provided by the smart cell information of the View Cell Space view (see [Displaying all services running on specific hosts, on page 2-51](#)).

Table 2-13: Links to Smart Cell Groups for Domain view

Origin	Link
System Status view, on page 2-20	domain name (Smart Cell Group Information)

Table 2-14: Links from Smart Cell Groups for Domain view

Destination	Link
System Status view, on page 2-20	Return to Summary

Application Management view

Use this view to start, stop, and restart one or more servers on the system.

This view is useful to show the start, stop, and pending status of a server. However, use this view only when necessary, such as when upgrading a host or before a planned power outage. This view should be used only by service personnel or administrators.

Table 2-15: Application Management view features

Feature	Description
server group title	Name of server group currently shown: <ul style="list-style-type: none">• ALL Systems: All server groups• MINING Servers: All email mining servers• HTTP Servers: All HTTP portal servers• SMTP Servers: All SMTP portal servers• META Servers: All metaservers• SMARTCELLS Server: All smart cell servers
Number	If ALL Systems is displayed: <ul style="list-style-type: none">• Number of server groups found in the system If specific server group is displayed: <ul style="list-style-type: none">• Number of hosts in specific group
Group Selection	Click one of the following buttons to select all server groups or a specific server group to affect: <ul style="list-style-type: none">• ALL Systems• MINING Servers• HTTP Servers• SMTP Servers• META Servers• SMARTCELLS PCC Servers and DB2 Servers are not available buttons because you should not perform actions on these servers separately. You must perform actions on these servers in a specific order, which you can perform only when performing an action on ALL Systems.
Status Area	Status of action performed.

Table 2-15: Application Management view features (continued)

Feature	Description
All Systems	<p>If ALL Systems is displayed, shows all server groups associated with the system.</p> <ul style="list-style-type: none"> • General status of server group. A check icon (✓) indicates normal operation. An X icon (✗) indicates one or more servers in group is down. An ! icon (!) indicates an action is pending. • Group name: <ul style="list-style-type: none"> – META Servers – SMARTCELLS Servers – MINING Servers – HTTP Servers – SMTP Servers – PCC Servers – DB2 Servers • Number of servers in group. • Group status (STARTED, STOPPED, STARTING, STOPPING, and PENDING).
Server Group	<p>If a specific server group is displayed, shows all hosts in group.</p> <ul style="list-style-type: none"> • General status of host. A check icon (✓) indicates normal operation. An X icon (✗) indicates one or more servers in group is down. • Host name. • IP address. • Host status (STARTED, STOPPED, STARTING, STOPPING, and PENDING).

Table 2-16: Links to Application Management view

Origin	Link
left menu	Application Management

Links from Application Management view: none

Starting, stopping, and restarting servers on the system

1. Click to select server group.
2. Click one of the following buttons:
 - **Start:** Start all systems or hosts in selected server group.
 - **Stop:** Stop all systems or hosts in selected server group.
 - **Restart:** Stop and immediately start all systems or hosts in selected server group.

User Management view (Dynamic Account Synchronization)

Use this view to configure Dynamic Account Synchronization (DAS) to automatically create and update email user accounts on Reference Information Storage System. You can define multiple configurations to extract various sets of users from one or more LDAP servers for specific Reference Information Storage System domains.

The basic flow for configuring DAS is as follows:

1. Click **New** under **LDAP Server Connection(s)** to set up connection to an LDAP server.
2. Click **Configuration** to name the DAS configuration and associate it to the LDAP connection set up in step 1.
3. For selected configuration, click **Job Mappings** to specify where DAS extracts users in the LDAP tree and where it adds or updates users on Reference Information Storage System.
4. Click **Job Assignments** to specify where and when selected DAS configuration runs.

Note: DAS does not support automatic deletion of user and remote authentication for Lotus Domino users. All users you import through DAS are local and have empty passwords. Use Platform Account Manager (PAM) to delete users.

Configuring DAS

1. In the User Management view, click **New** under **LDAP Server Connection(s)**.
2. Enter the following information:
 - In the **Server ID** field, enter name identifying server connection. For example, enter “server250” for the LDAP server 10.1.1.250. Name must be unique among other server connections on the system.

- In the Hostname field, enter IP address of LDAP server where user information is located.
- In the Port field, enter LDAP server port that DAS uses. The default is 389.
- In the Binder user field, enter user ID with administrative privileges on the LDAP server.

You might want to create a user profile on the LDAP server specifically for DAS use. Include the domain in this entry. For example, for a user named `dasUser` and domain `ldaptest.com`, enter `cn=dasUser,cn=Users,dc=ldaptest,dc=com`. The default user ID is Administrator (`cn=Administrator,cn=Users,dc=ldaptest,dc=com`).

For Domino configuration, you must enter a binder that has access and rights to read the LDAP directory on the HP Gateway. The gateway administrator user can be used for this purpose or a user with equivalent rights.

- In the Binder pswd field, enter password associated with binder user.
3. Click New. The system attempts to validate connection and displays a message when configuration is created.
 4. Return to the User Management view, and click Configuration. The Configuration view appears.
 5. Click Create. The New Configuration name box appears.
 6. Enter name identifying configuration. Do not use spaces or dashes, but underscores are allowed.
 7. Click Add.
 8. Return to the Configuration view, and click the option button next to the existing DAS configuration to associate with an LDAP server.
 9. Click Server. A new view displays available DAS configurations and server connections.
 10. Select configuration and server connection from the list. Multiple DAS configurations can be associated with the same server connection.

For Domino configuration, you must choose the Lotus Domino as the server category. This sets the environment for DAS.

11. Click Associate.
12. Return to the User Management view, and click Job Mappings. The Job Mappings view appears.
13. Click Create. A mapping entry form is displayed, or a message informs you there are no configurations to be mapped.
14. Enter the following information:

Table 2-17: User Management view, job mappings form

Field	Description
Configuration ID	DAS configuration that uses this mapping. Select desired configuration from the pull-down list.
Source LDAP Domain name	Domain on LDAP server where user accounts are to be monitored. For example, enter <code>ldaptest.com</code> .
Starting Point	Root node where user accounts are stored on the LDAP server. For example, enter <code>cn=Users,dc=ldaptest,dc=com</code> for node Users in domain <code>ldaptest.com</code> . Value must specify relative location in the LDAP tree, including parent nodes and domain name. For Domino configuration, set the Starting Point to blank to mine all aggregated Domino domain/organizations.
Update LDAP filter	Criteria to include or exclude specific users. Use at least the default, <code>(objectclass=user)(mail=*)</code> , which excludes users who do not have email accounts.
LDAP Query return attributes	Use this field to specify the list of return attributes. <ul style="list-style-type: none"> • For Exchange, use the default attributes unless your LDAP schema requires mapping changes. • For Domino, the list of return attributes is set to the following by default: <code>uid,sn,modifytimestamp,createtimestamp,cn,give nName,mail,sn,dominouid,dominodn</code>

Table 2-17: User Management view, job mappings form (continued)

Field	Description
USNChanged	<p>Active Directory's unique sequence number (USN) the last time DAS ran. Active Directory increments the USN for each change in any of its user accounts. When DAS finds a larger USN, it extracts new information. For initial Reference Information Storage System setup, set USNChanged to "1" so DAS extracts all users. Thereafter, do not change this value.</p> <p>To change this value, stop all scheduled jobs for this DAS configuration. Use the Configuration Command Panel in the Job Assignments view (see Starting or scheduling DAS jobs, on page 2-34).</p>
Target appliance Domain ID	ID (not name) of Reference Information Storage System domain where users are synchronized with users on the LDAP server.
NextRepID	<p>RISS repository ID assigned to new users. DAS retrieves this value from the database, but you can use this feature to specify the repository ID for the first user inserted when DAS runs. For example, if you enter 67, the repository created and assigned for the first imported user is R0000067. You can use this feature if users already exist in the system or to reserve repository IDs for any reason. If you specify a value that is lower than an existing repository ID, DAS automatically changes the value to the next higher number.</p> <p>To change this value, stop all scheduled DAS configurations that import users to the domain to which the specified repository belongs. Use the Configuration Command Panel in the Job Assignments view (see Starting or scheduling DAS jobs, on page 2-34).</p>
DeleteStartingPoint	Root node where deleted user objects are stored on the LDAP server. For example, enter <code>cn=deletedObjects,dc=ldaptest,dc=com</code> for node <code>deletedobjects</code> in domain <code>ldaptest.com</code> . Value must specify relative location in the LDAP tree, including parent nodes and domain name.
Delete LDAP Filter	Criteria to include or exclude specific users in the LDAP deleted users directory. Add to the default for special cases.

Table 2-17: User Management view, job mappings form (continued)

Field	Description
Delete USNChanged	USN in deleted users directory the last time DAS ran. For initial Reference Information Storage System setup, set this value to "0". Thereafter, do not change this value. To change this value, stop all scheduled jobs for this DAS configuration. Use the Configuration Command Panel in the Job Assignments view (see Starting or scheduling DAS jobs, on page 2-34).

15. Click Update.
16. Return to the User Management view, and click Job Assignments. The Job Assignments view appears.
17. Click Create. An entry form appears.
18. In the ConfigID list, select DAS configuration to be run on the portal.
19. In the DAS Server IP field, enter IP address of HTTP portal where the DAS service runs selected DAS configuration.
20. Select Yes for Configuration Enabled.
21. In the Period (mn) field, enter number of minutes to occur between runs of selected DAS configuration. A period of 0 means the job runs once.
22. Do not change the defaults for the Configuration running state and DAS server running state fields. These fields are for future use.
23. Click Update.
24. In the Configuration Command Panel, select Yes for Initialize DAS setup.

Select Yes only when scheduling or starting DAS configuration for the first time, or to resynchronize the database to recover from an unusual event.
25. Click Start to run DAS configuration immediately.
26. After DAS updates the database, go to the Configuration Command Panel, and select No for Initialize DAS setup.
27. Click Schedule to run DAS configuration periodically.

Updating connections to LDAP servers

1. In the User Management view, under the LDAP Server Connection(s) section, click the option button next to the existing LDAP server connection.
2. Click Update. A new view displays current host, port, user, and password.
3. Type new values as needed. To clear all values, click Reset before entering new data.
4. Click Update.

Deleting connections to LDAP servers

1. In the User Management view, under the LDAP Server Connection(s) section, click the option button next to the existing LDAP server connection.
2. Click Delete.

Displaying DAS configuration associations

1. In the User Management view, click Configuration.
2. Click the option button next to the existing DAS configuration.
3. Click Server to show which LDAP server is associated with selected DAS.

Deleting DAS configuration associations

1. In the User Management view, click Configuration.
2. Click the option button next to the existing DAS configuration.
3. Click Delete.

Updating or deleting mappings

1. In the User Management view, click Job Mappings.
2. To update the mapping, locate the configuration, change the job mapping form, and click Update below the form.

3. To delete the mapping, locate the configuration, and click **Delete** below the form.

Note: If there is more than one configuration, be sure to click the correct **Update** or **Delete** button. If you do not, the wrong mapping might be updated or deleted.

Updating or deleting assignments

1. In the User Management view, click **Job Assignments**.
2. To update the assignment, locate the configuration, change the job mapping form, and click **Update** below the form.
3. To delete the assignment, locate the configuration, and click **Delete** below the form.

Note: If there is more than one configuration, be sure to click the correct **Update** or **Delete** button. If you do not, the wrong assignment might be updated or deleted.

Starting or scheduling DAS jobs

1. In the User Management view, click **Job Assignments**.
2. In the Configuration Command Panel, locate the correct configuration, and do one of the following:
 - Click **Start** to run configuration immediately.
 - Click **Schedule** to run configuration periodically as specified in assignment values.

Displaying servers with assigned DAS configurations

The Web Servers and Assignments area of the User Management view lists HTTP servers with their assigned DAS configurations. Click a DAS configuration. The Job Assignments view appears, where you can view, change, delete, or start and stop the configuration.

Smartcell Cloning view

This view shows status of current and past cloning operations. Use this view to clone a smart cell. You can clone a smart cell if its mirror smart cell is SUSPENDED, DEAD, or FAILED. (See [Smart cell life cycle states, on page 2-13.](#))

Cloning a smart cell copies all its information to another smart cell that is in the FREE state to give the smart cell a new, viable mirror. Cloning operations can take a long time (even a day) depending on amount of information cloned.

When you access the Smartcell Cloning view, PCC searches for ongoing cloning operations and loads current data. Only one smart cell can be cloned at a time, so you see the progress of any ongoing cloning operation.

Table 2-18: Smartcell Cloning view features

Feature	Description
Cloning Set up	<p>Smart cells whose mirrors are not viable and how many free cells are available.</p> <ul style="list-style-type: none">• Source: IP address of smart cell without viable mirror. If all smart cells have viable mirrors, displays “No Broken Groups Found.” If more than one smart cell needs a mirror, a Change Source button appears below the automatically selected IP address.• Free Cells: Number of smart cells currently in the FREE state. This is decremented by one after a cloning operation starts.
Clone Cell	<p>Starts cloning operation. See Cloning smart cells (copying data), on page 2-38.</p>

Table 2-18: Smartcell Cloning view features (continued)

Feature	Description
Status Area	<p>The following information about an ongoing cloning operation:</p> <ul style="list-style-type: none"> • Source selected: IP address of smart cell being duplicated. • Target selected: IP address of smart cell receiving duplicate data. • Current Step Percentage: Dynamic bar showing how much source data has been duplicated. • Overall Percentage: Current step in cloning operation. Steps are Initializing, Assigning target host, Transferring data, Transferring indexes, Waiting for indexer to complete, Updating history log, and Completed or Failed. Some steps happen so quickly you may not see them. Steps such as Transferring data and Transferring indexes can take a long time if there is much data to clone.
History Logs	<p>The following information about each cloning operation that has occurred since startup:</p> <ul style="list-style-type: none"> • Source • Target • Time Elapsed • Status • Date

Table 2-19: Links to Smartcell Cloning view

Origin	Link
left menu	Smartcell Cloning

Links **from** Smartcell Cloning view: none



See Also

- [Smart cell life cycle states, on page 2-13](#)

Cloning smart cells (copying data)

1. Select smart cell from the Source field.

Note: Click Change Source, when present, to select a different smart cell for cloning. When the selection box appears, select the desired smart cell from the pull-down list, and click Select.

2. Click Clone Cell. This button is unavailable if there are no smart cells to clone.
3. Check the Status Area to see results of cloning operation. The check icon () indicates cloning operation is proceeding normally. If the operation fails, an X icon () appears.

Replication view

Note: This view is available only if a replicated system is configured.

Use this view to monitor and start or stop replicating a domain on a remote system. Replication status is updated after each polling cycle, so it could be up to 5 minutes after you start replication before you see results on the graph of replication rates. Errors and warnings, however, are displayed as soon as they happen on the system. (The Replication view is unavailable until at least one domain on the PCC host system is configured for replication.)

A failed replicated smart cell triggers allocation of new primary and secondary smart cells on the replica site. When the original site returns to service, it automatically becomes the replica site for new primary and secondary smart cells. Depending on configuration, some administration may be necessary for continued data storage. Specifically, if the system uses Selective Archiving, the replica site mining servers must be configured and enabled to start mining to the replica site.

If the primary site is not available for queries, end users must enter address of the replica site, instead of primary site, in their browsers.

Table 2-20: Replication view features

Feature	Description
Domain Information	<p>For each domain configured for replication:</p> <ul style="list-style-type: none">• Domain Name: DNS name of domain.• Service: Whether replication is in progress (Running) or not (Stopped).• Between: Names of local and replication systems. First system named is the domain location. Second system named is the remote system where domain is being replicated.• Current Transfer Rate: How many messages and documents are being duplicated per second.• Current Percentage of Data Replicated: How much data currently stored in domain has been duplicated.

Related Views

- [Displaying all services running on specific hosts, on page 2-51](#)
- [Smartcell Cloning view, on page 2-36](#)

Table 2-21: Links to Replication view




Origin	Link
left menu	Replication

Links from Replication view: none

Displaying replication statuses for groups in a domain and replication performance over time

Click Details.

For each group in domain, detail view shows:

- Status, name, and total messages of group on local system. A check icon () indicates normal operation, an X icon () indicates replication failed last time it was tried, and an ! icon () indicates replication is being retried.
- An arrow showing direction of data between groups. Normally, direction is left to right, from group on local host to group on remote host. In a failover situation, direction is right to left, as data replicated on remote host is being used to restore group on local host.
- Name and total messages of replication group.
- How much data in source group has been copied to destination group.

A graph shows number of messages stored per second on local and replication (remote) systems for selected domain. You can select last year, last month, last 24 hours, or last hour to graph.

Starting replication for specific domains

Click START NOW below domain information. Replication will replicate batch that was next when it stopped.

Stopping replication for specific domains

Click STOP NOW below domain information. Replication will stop after current batch is replicated.

Selective Archiving folder

Mining Overview view

This view provides status information about the mining system for each domain. It shows information about Exchange server, mining server, and system; and mining system information about host and service status. In addition, this view provides graphical store rate information. If selective archiving is not available or running, an error message is displayed.

Table 2-22: Mining Overview view features



Feature	Description
Exchange Server	<p>Information about Exchange server and its status.</p> <p>For servers with more than one domain, choose domain from the pull-down list.</p> <p>For each domain:</p> <ul style="list-style-type: none">• Server host name or IP address.• General status of Exchange server. A check icon () indicates normal operation. An X icon () indicates a problem or inactive service.• Name and size of mailbox.• Number of items.

Table 2-22: Mining Overview view features (continued)







Feature	Description
Mining Server	<p>Information about mining server and its status.</p> <ul style="list-style-type: none"> • Server host name or IP address. • General status of mining server. A check icon () indicates normal operation. An X icon () indicates a problem. An ! icon () indicates mining has stopped. • Number of journal and mailbox miners. • Rate and number of stored journal items. • Number of rejected items. • Number of stubs created. A stub is a representation of original email that has been mined. • Number of stored email items.
Appliance	<p>Information about RISS and its status.</p> <ul style="list-style-type: none"> • Server host name or IP address. • General status of the system. A check icon () indicates normal operation. An X icon () or ! icon () indicates a problem or inactive service. • Domain names. • Rate and number of stored items. • Number of SMTP portals.

Table 2-22: Mining Overview view features (continued)

Feature	Description
Mining System Info	<p>Host and service status information about mining system.</p> <ul style="list-style-type: none"> • Host name and IP address. • Host sending mode. INTERNAL is the default and indicates data is being sent directly to RISS. EXTERNAL indicates data is being sent to memory before reaching RISS. RELAY indicates a mix of internal and external sending modes are occurring. UNKNOWN indicates a potential problem. • Status of Jboss, Mail Attender, and Miner Manager services. • Status of journal and mailbox TNEF services (ON or OFF).
Historical Store Rate graph	<p>Graph showing number of messages per second each domain on the system stored in given specified time frame. The default shows storage rate in last hour, ending with current time. Click Last 24 Hours, Last Month, or Last Year to change time period.</p>

Table 2-23: Links to Mining Overview view

Origin	Link
left menu	Mining Overview

Links **from** Mining Overview view: none

Stopping mining servers

Click STOP NOW below server information. Based on number of servers, there is a latency period when stopping servers.

Note: You can also stop the mining server from the Application Management view.

Starting mining servers

Click START NOW below server information. Based on number of servers, there is a latency period when starting servers.

Note: You can also start the mining server from the Application Management view.

Miner 1

Use the Miner1 link on the left menu to access VNC. Use VNC to access the email miner through PCC. More than one email miner might be available.

System Backup view

Note: This view is available only if a backup system is configured.

Access this view from the System Backup left menu item. This view provides information about the status of backup servers, signature backups, and data backups, and direct access to a Tivoli Server Administration web client.

Use the backup feature to back up all archived messages, documents, and digital signatures to write-once-read-many times (WORM) media, including optical media. This feature provides:

- additional level of data reliability for exceptional cases where all smart cells in a group fail simultaneously
- disaster recovery of system data

The backup daemon copies data in batches from RISS smart cells once every hour or so.

Compared to message and document backups, signature backups save space and are quicker. Use signature backups to meet compliance requirements for determining if archived documents are corrupt. It does *not* back up messages or documents. If the system configuration provides signature backup duplication, a second backup copy of each signature is created. Both backup copies are produced by primary and duplicate signature backup services.

The System Backup view contains tabbed panels: Overview, Signatures, and Data Backup. Click on a panel to view the system status for that item.

Table 2-24: Overview panel features, System Backup view




Feature	Description
Backup Status	<p>For each backup server:</p> <ul style="list-style-type: none"> • General status of backup server and each of its services. <p>Check icons () indicate normal operation; X icons () or ! icons () indicate a problem or inactive service.</p> <ul style="list-style-type: none"> • Remote Administration: Click Tivoli Console to access the Tivoli Server Administration web client, providing remote access to Tivoli servers used for backup. • Summary of active group backup status. • For each backup library on the server, number of volumes and free volumes in the library. A backup library is a collection of backup volumes.
Alerts & Warnings	For each backup server, alerts and warnings currently in effect.

Table 2-25: Signatures panel features, System Backup view

Feature	Description
Signatures backed up	Proportion of signatures backed up, expressed as a percentage and as a ratio of total number of signatures.
Primary Signature Server	<p>Status of primary signature backup services:</p> <ul style="list-style-type: none"> • Server Name: Server (Internal or External) where primary signature backup services run • Library: Name of library for primary signature backups • Last Backup: How long ago last primary signature backup occurred • Space Occupied: Number of megabytes of storage used for primary signature backup • Volumes: Names of primary signature backup volumes, and how full they are (percentage)
Duplicate Signature Server	Same as Primary Signature Server, substituting “duplicate” for “primary.”

Table 2-26: Data Backup panel features, System Backup view

Feature	Description
Library	Name of library for data backups. A backup library is a collection of backup volumes.
Server Name	Server (Internal or External) where data backup services run.
Files backed up	<ul style="list-style-type: none"> Proportion of files backed up, expressed as a percentage and as a ratio of total number of files. Graph of percentage of data files backed up over last 24 hours.
Active Groups	<p>For each group (pair) of active smart cells (<i>not</i> closed or suspended):</p> <ul style="list-style-type: none"> Domain name and IP address of smart cell used for backup (usually secondary smart cell) Unique smart cell group identification number Percentage and number of data files, and total number of files Time since last backup cycle: How long ago last data backup occurred Group/Backup Daemon Status: State of smart cell being backed up, and backup daemon (process) status Space Occupied: Number of megabytes of storage used to back up data Volumes: Names of backup volumes, and how full they are (percentage)
Inactive Groups	Same as Active Groups, but for inactive groups (closed or suspended smart cells)

See Also

- Tivoli/IBM web site: <http://www.ibm.com/software/tivoli/>
- Smart cell life cycle states, on page 2-13*

Table 2-27: Links to System Backup view

Origin	Link
left menu	System Backup

Links **from** System Backup view: none

Checking status of backups

Click System Backup on the left menu.

Accessing Tivoli Server Administration web client

Click Tivoli Console to access the Tivoli Server Administration web client. See the Tivoli documentation for more information. Also, see the RISS 1.1 release notes for late-breaking issues.

Monitoring folder

Tactical Monitoring view

This view provides a high-level summary of system status (health) and monitoring services. Use this view to enable or disable individual monitoring features.

This view shows how many hosts and services have each status value and how many problems are acknowledged and unacknowledged (unhandled). Use other views to investigate these problems further.

Table 2-28: Tactical Monitoring view features

Feature	Description
Monitoring Performance	<p>Current performance of monitoring processes:</p> <ul style="list-style-type: none"> • Check Execution Time: Minimum, maximum, and average times to execute a monitoring check • Check Latency: Minimum, maximum, and average durations between time a monitoring check was scheduled and time it was executed • # Active Checks: How many services are monitored • # Passive Checks: Currently <i>not used</i> (all checks are active)
Network Health	Average health of all hosts and services. Green indicates normal operation; red indicates one or more components stopped or failed; yellow indicates potential problems (warning). See Host and service status values , on page 2-14, for more information.
Hosts	Number of hosts with each host status value.
Services	Number of services with each service status value.
Monitoring Features	Indicates if Notifications and Active Checks are enabled. (RISS <i>does not use</i> Flap Detection; or Event Handlers and Passive Checks, which are enabled by default.)

Related Views

- The charts Hosts and Services in the Tactical Monitoring repeat information available in the charts Host Status Totals and Service Status Totals in other views. See [Status Summary view](#), on page 2-17.

- The following views provide more information about monitoring performance:
 - [Scheduling Queue view, on page 2-73](#)
 - [Hostgroup Information view, on page 2-121](#)
- Use the command Acknowledge this host/service problem in the Host/Service Information view to acknowledge host and service problems. See [Example: Acknowledging problems, on page 2-144](#).

Table 2-29: Links to Tactical Monitoring view

Origin	Link
left menu	Tactical Monitoring

Table 2-30: Links from Tactical Monitoring view

Destination	Link
Scheduling Queue view, on page 2-73	Monitoring Performance
Service Detail view, on page 2-53 , for all hosts or services with specific status value	host or service status value
External Command Interface view, on page 2-143	Enabled/Disabled

Displaying all services running on specific hosts

In the Tactical Monitoring view, under Hosts, click number of hosts with given status value, for example 2 DOWN. The Service Status Details view appears. See [Service Detail view, on page 2-53](#), for more information.

Displaying problem status of specific hosts

Hosts with problem status values are divided into those with acknowledged problems and the rest (unhandled).

In the Tactical Monitoring view, click one of the following links:

- <#> Acknowledged

- <#> Unhandled Problems

The Service Status Details view appears. See [Service Detail view, on page 2-53](#), for more information.

See [Example: Acknowledging problems, on page 2-144](#), for information about acknowledging problems.

Displaying service status of specific services

In the Tactical Monitoring view, under Services, click number of services with a given status value, for example 3 CRITICAL. The Service Status Details view appears. See [Service Detail view, on page 2-53](#), for more information.

Displaying problem status of specific services

Services with problem status values are divided into those with acknowledged problems, those running on hosts that are DOWN, and the rest (unhandled).

In the Tactical Monitoring view, click one of the following links:

- <#> Acknowledged
- <#> on Problem Hosts (DOWN)
- <#> Unhandled Problems

The Service Status Details view appears. See [Service Detail view, on page 2-53](#), for more information.

See [Example: Acknowledging problems, on page 2-144](#), for information about acknowledging problems.

Enabling or disabling features

1. In the Tactical Monitoring view, click Enabled/Disabled for any listed monitoring feature, such as Event Handlers. The External Command Interface view appears.
2. Disable or enable the feature. See [Example: Enabling or disabling notifications, on page 2-144](#), for more information.



Service Detail view

This view provides detailed service information for a specific host, all hosts in a host group, or all hosts in the system.

The charts Host Status Totals and Service Status Totals of the Service Detail view are the same as those of the Status Summary view with the following exception: Clicking a status value column heading in the chart Host Status Totals displays the Service Status Details view, filtered to show only services running on hosts with that host status value (it does *not* display the Service Overview view). See [Status Summary view, on page 2-17](#), for more information.

The chart Service Detail provides information about services running on target hosts. Some chart column headings have associated vertical arrows. To sort the chart in ascending order for a given column, click the orange up arrow; to sort in descending order, click the green down arrow.

Table 2-31: Service Status Detail view, Service Status Details chart features

Feature	Description
Host	Target hosts. Color coding indicates host health. See Host and service status values, on page 2-14 . Icons indicate presence of comments () and/or scheduled downtimes ().
Service	Services running on each target host. Color coding indicates service health. See Host and service status values, on page 2-14 .
Status	Current status values of services. See Host and service status values, on page 2-14 .
Last Check	Time service was last checked.
Duration	Length of time service has been running.
Attempt	Number of successful attempts and total number of attempts to check service.
Status Information	Additional information about service health.

Related Views

- The Service Problems view is a subset of the Service Status Details view, providing information about only services that have problems. See [Service Problems view, on page 2-61](#).

Table 2-32: Links to Service Status Details view

Origin	Link
left menu	Service Detail
Status Summary view, on page 2-17	<ul style="list-style-type: none"> • View Service Status Detail . . . • status column heading, Service Status Totals chart (services with that status value) • host status value in chart Status Summary For All Host Groups (services running on hosts with that status value) • service status value in chart Status Summary For All Host Groups (services with that status value)
Host Detail view, on page 2-56	<ul style="list-style-type: none"> • View Service Status Detail . . . • status column heading, chart Service Status Totals (only services with that status value)
Host Problems view, on page 2-62	<ul style="list-style-type: none"> • View Service Status Detail . . . • status column heading, chart Service Status Totals (only services with that status value)
Service Overview view, on page 2-58	<ul style="list-style-type: none"> • View Service Status Detail . . . • status column heading, chart Service Status Totals (services with that status value) • host name, or host status-signal icon () , chart Service Overview . . . • Services entry, chart Service Overview . . .
Status Grid view, on page 2-141	<ul style="list-style-type: none"> • View Service Status Detail . . . • status column heading, chart Service Status Totals (services with that status value) • host group name, chart Status Grid For . . . • host status-signal icon () , chart Status Grid For . . .
Alerts folder, on page 2-94, for host trends	View Status Detail For This Host

Table 2-32: Links to Service Status Details view (continued)

Origin	Link
Availability view, on page 2-85 , for single host	View Status Detail For This Host
Creating availability reports, on page 2-88	View Status Detail For This Host
Alerts History view, on page 2-97	View Status Detail . . .
Notifications view, on page 2-89 , for single host or when gray-box heading is Notifications	View Status Detail . . .
Service Problems view, on page 2-61	<ul style="list-style-type: none"> • View Host Status Detail . . . • status column heading, Host Status Totals chart (only services running on hosts with that host status value)
Hostgroup Information view, on page 2-121	View Status Detail For This Hostgroup
Service Information view, on page 2-133	View Status Detail For This Host
Host Information view, on page 2-126	View Status Detail For This Host
Tactical Monitoring view, on page 2-50	specific status values for hosts or services
Scheduling Queue view, on page 2-73	Active Service Checks (<#> Total)
Scheduling Queue view, on page 2-73	specific service name
Service Status Details	status column heading, chart Host Status Totals (only services running on hosts with that host status value)
Service Detail	status column heading, chart Service Status Totals (only services with that service status value)

Table 2-33: Links from Service Detail view

Destination	Link
Service Information view, on page 2-133	service name
When main heading is Service Status Details For . . . <hostgroup(s)>	
Status Summary view, on page 2-17	View Host Status Summary . .
Host Detail view, on page 2-56	View Host Status Detail . .
Service Overview view, on page 2-58	View Service Overview . .
Status Grid view, on page 2-141	View Host Status Grid . .
When main heading is Service Status Details For All Hosts	
Alerts History view, on page 2-97	View History For All Hosts
Notifications view, on page 2-89	View Notifications For All Hosts
Host Detail view, on page 2-56	View Host Status Detail For All Hosts

Displaying status information for specific hosts

Under Host, click host name, such as sc-sc1-172-1. See [Host Information view, on page 2-126](#).

Display status information for specific services



Under the Service column, click service name, such as PING. See [Service Information view, on page 2-133](#).

Host Detail view

The charts Host Status Totals and Service Status Totals of this view are the same as those of the Status Summary view. See [Status Summary view, on page 2-17](#).

The chart Host Status Details provides status information about a specific host, all hosts in a host group, or all hosts in the system. Some chart column headings have associated vertical arrows. To sort the chart in ascending order by a given column, click the orange up arrow; to sort in descending order, click the green down arrow.

Table 2-34: Host Detail view, Host Status Details chart features

Feature	Description
Host	Target hosts. Icons indicate presence of a comments () and/or scheduled downtimes ().
Status	Current host status values. See Host and service status values, on page 2-14 .
Last Check	Time host was last checked.
Duration	Length of time host has been running.
Status Information	Additional information about host status.

Related Views

- The Host Problems view is a subset of the Host Detail view, providing information about only hosts that have problems. See [Host Problems view, on page 2-62](#).

Table 2-35: Links to Host Detail view

Origin	Link
left menu	Host Detail
Status Summary view, on page 2-17	View Host Status Detail . . .
Service Detail view, on page 2-53 , when main heading is Service Status Details For . . . <hostgroup(s)>	View Host Status Detail . . .
Service Overview view, on page 2-58	View Host Status Detail . . .
Status Grid view, on page 2-141	View Host Status Detail . . .
Scheduling Queue view, on page 2-73	host name

Table 2-36: Links from Host Detail view

Destination	Link
Service Detail view, on page 2-53	View Service Status Detail . . .
Service Overview view, on page 2-58	View Service Overview . . .
Status Summary view, on page 2-17	View Status Summary . . .
Status Grid view, on page 2-141	View Status Grid . . .
Hostgroup Information view, on page 2-121	host group abbreviation, in parentheses, such as (sc)

Displaying status information for specific hosts

In the Host column, click host name, such as sc-sc1-172-1. See [Host Information view, on page 2-126](#).

Service Overview view

Use this view to see the status of each host in a single host group or all host groups. For each host, this view shows number of services that have each service status value.



The charts Host Status Totals and Service Status Totals are the same as those of the Status Summary view. See [Status Summary view, on page 2-17](#).

The chart Service Overview For <hostgroup(s)> provides information about status values of hosts and services in displayed host groups.

Table 2-37: Service Overview view features

Feature	Description
chart title	Host group name (for example, Smart Cells) and its abbreviation (for example, sc). Click chart title to open the host group's Service Detail view.
Host	Hosts in host group.
Status	Host's current status value. See Host and service status values, on page 2-14 .

Table 2-37: Service Overview view features (continued)

Feature	Description
Services	Number of services running on host having each status value (counts of zero are omitted). For example, 6 OK means six services are functioning correctly.
Actions (two buttons):	
<ul style="list-style-type: none"> View Extended Information For This Host () 	<ul style="list-style-type: none"> Displays host's Host Information view. See Host Information view, on page 2-126.
<ul style="list-style-type: none"> View Service Details For This Host () 	<ul style="list-style-type: none"> Same as clicking host name (see Host, previous row).

Related Views

- The Status Summary view information is a subset of the Service Overview view information. The Status Summary view provides only the number of hosts having each status value. See [Status Summary view, on page 2-17](#). The Service Overview view provides status value of each host. Use the Service Overview for information about individual hosts.

Table 2-38: Links to Service Overview view

Origin	Link
left menu	Service Overview
Status Summary view, on page 2-17	<ul style="list-style-type: none"> View Service Overview . . . host group name (overview of that host group) status column heading, Host Status Totals chart (overview of that status value for all host groups)
Host Detail view, on page 2-56 , and Host Problems view, on page 2-62	<ul style="list-style-type: none"> View Service Overview . . . status column heading, Host Status Totals chart (overview of that status value for all host groups)
Service Detail view, on page 2-53 , when main heading is Service Status Details For . . . <hostgroup(s)>	View Service Overview . . .

Table 2-38: Links to Service Overview view (continued)

Origin	Link
Status Grid view, on page 2-141	<ul style="list-style-type: none"> • View Service Overview . . . • status column heading, Host Status Totals chart (overview of that status value for all host groups)
Hostgroup Information view, on page 2-121	View Service Overview For This Hostgroup
Service Overview	status column heading, Host Status Totals chart (overview of that status value for all host groups)


Table 2-39: Links from Service Overview view

Destination	Link
Service Detail view, on page 2-53	View Service Status Detail . . .
Host Detail view, on page 2-56	View Host Status Detail . . .
Status Summary view, on page 2-17	View Status Summary . . .
Status Grid view, on page 2-141	View Status Grid . . .

Displaying host groups


1. Scroll to the bottom of the Service Overview view.
2. Find the host group's chart, and click the host group's name above the chart; for example, Routers for Smart Cells (cr). The Service Status Details for Host Group view appears.

Displaying service status of specific hosts

1. Scroll to the bottom of the Service Overview view.
2. Find the host's host group.
3. In the Actions column, click View Service Details For This Host ().
- OR -
In the Host column, click host name; for example, sc-sc1-172-1.

The Service Status Details view appears. See [Service Detail view, on page 2-53](#), for more information.

Displaying host information for specific hosts

1. Scroll to the bottom of the Service Overview view.
2. Find host's host group.
3. In the Actions column, click View Extended Information For This Host (). The Host Information view appears. See [Host Information view, on page 2-126](#), for more information.

Displaying status values for specific hosts and services

1. Scroll to the bottom of the Service Overview view.
2. Find host's host group.
3. In the Services column, click an entry, such as 6 OK. The Service Status Details view appears. See [Service Detail view, on page 2-53](#), for more information.

Service Problems view

This view is a subset of the Service Detail view, providing information about only services that have problems. See [Service Detail view, on page 2-53](#).

See Also

- [Detailed email reports, on page 2-77](#), for information about automatically sending email reports containing the same information as the Service Problems view.

Table 2-40: Links to Service Problems view

Origin	Link
left menu	Service Problems
Status Summary view, on page 2-17	All Problems, in chart Host Status Totals or Service Status Totals

Table 2-40: Links to Service Problems view (continued)

Origin	Link
Service Detail view, on page 2-53	All Problems, in chart Host Status Totals or Service Status Totals
Service Overview view, on page 2-58	All Problems, in chart Host Status Totals or Service Status Totals
Status Grid view, on page 2-141	All Problems, in chart Host Status Totals or Service Status Totals
Host Detail view, on page 2-56	All Problems, in chart Service Status Totals

Table 2-41: Links from Service Problems view

Destination	Link
Alerts History view, on page 2-97	View History For All Hosts
Notifications view, on page 2-89	View Notifications For All Hosts
Service Detail view, on page 2-53	View Host Status Detail For All Hosts
Service Information view, on page 2-133	service name

Host Problems view

This view is a subset of the Host Detail view, providing information about only hosts that have problems. See [Host Detail view, on page 2-56](#).

See Also

- [Detailed email reports, on page 2-77](#), for information about automatically sending email reports containing the same information as the Host Problems view.

Table 2-42: Links to Host Problems view

Origin	Link
left menu	Host Problems

Table 2-43: Links **from** Host Problems view

Destination	Link
Service Detail view, on page 2-53	View Service Status Details For All Host Groups
Service Overview view, on page 2-58	View Service Overview For All Host Groups
Status Summary view, on page 2-17	View Status Summary For All Host Groups
Status Grid view, on page 2-141	View Status Grid For All Host Groups

Comments view

Comments are notes you make to yourself or other system administrators. This view displays all current host and service comments. Use this view to add or delete comments. The gray-box heading for this view is All Host and Service Comments.

Related Views

- [Host Information view, on page 2-126](#), lets you view, add, and delete comments for given host.
- [Service Information view, on page 2-133](#), lets you view, add, and delete comments for given service.


Table 2-44: Links **to** Comments view

Origin	Link
left menu	Comments

Table 2-45: Links **from** Comments view


Destination	Link
External Command Interface view, on page 2-143	Add a new host/service comment

Adding service or host comments


1. In the Service Comments or the Host Comments section, click the Add new service comment or the Add new host comment link (). The External Command Interface appears.
2. In the Command Options section, enter the following information:
 - Host Name
 - Service (if you are adding a service comment)

Note: Enter host and service names exactly as they appear in PCC views.

- Author (Your Name)
 - Comment
3. To retain comments between Nagios restarts, click to select the Persistent check box.
 4. Click Commit to save changes, or click Reset to clear input fields.

A cloud-callout icon () appears next to host or service entry in various views, such as Service Status Details.

Deleting comments

1. Find comment.
2. In the Actions column, click the wastebasket icon (). The External Command Interface appears.
3. In the Command Options section, enter the following information:
 - Host Name
 - Service
4. Click Commit to save changes, or click Reset to clear input fields.

Host Downtime view

Use this view to display and schedule host and service downtimes, and disable notifications during periods when target hosts and services are down. Scheduled downtimes are generally periods of planned outage. You can also schedule downtime for a host or service that is already down.

Note: The only effect of a scheduled downtime is to suppress sending notifications; in particular, services are *not* disabled during downtimes.

Since services are not disabled during downtimes, scheduling a downtime for a host also schedules equivalent downtimes for all its services. When a host is down, its service checks fail, causing the host itself to be checked. A detected host failure leads to a single notification about host being down; no service notifications are produced. If the host is scheduled for a downtime, host notification is suppressed; no notifications are sent.

Scheduled downtimes are preserved across PCC shutdowns and restarts.

Related Views

- [Host Information view, on page 2-126](#), lets you schedule and delete scheduled host downtime.
- [Service Information view, on page 2-133](#), lets you schedule and delete scheduled service downtime.
- [Scheduling Queue view, on page 2-73](#), displays scheduled host and service checks, and lets you schedule checks.
- [Nagios Info view, on page 2-68](#), lets you disable notifications for all hosts and services. This is *not* for a limited period, however. Notification remains globally disabled until you re-enable it.

Table 2-46: Links to Host Downtime view

Origin	Link
left menu	Host Downtime

Table 2-47: Links from Host Downtime view

Destination	Link
External Command Interface view, on page 2-143	Schedule host/service downtime

Disabling notifications by scheduling service or host downtimes

1. In the Scheduled Service Downtime or the Scheduled Host Downtime section, click Schedule service downtime or Schedule host downtime. The External Command Interface appears.
2. In the Command Options section, enter the following information:
 - Host Name
 - Service (appears in the Schedule service downtime only)
 - Author (Your Name)
 - Comment
 - Start Time
 - End Time


Note: Fields in red, including Comment, are required. If you do not enter a comment, you are informed that “an error occurred while processing your command.”

3. To limit downtime to specified start and end times, click to select the Fixed check box.


To use flexible downtime for service, leave the Fixed check box unselected, and enter information in the Duration fields.

Note: When Fixed is not selected, scheduled downtime is flexible: it starts between specified start and end times as soon as a problem is detected (UNREACHABLE or DOWN status value for host, non-OK for service).

4. Click Commit to save changes, or click Reset to clear input fields.

A snore icon () appears next to host or service entry in various views, such as Service Status Details.

Re-enabling notifications by deleting scheduled downtimes

1. Find downtime.
2. In the Actions column, click the wastebasket icon (). The External Command Interface view appears.
3. Click Commit to save changes, or click Reset to clear input fields.

Nagios folder

Nagios Info view

This view provides information about Nagios, the PCC process monitoring hosts and services. The gray-box heading for this view is Nagios Process Information.

PCC *does not use* several features of this view. Only features that PCC uses are described.

Program Information chart

Table 2-48: Program Information chart, Nagios Info view

Variable	Description
Program Start Time	Time PCC started.
Total Running Time	Length of time PCC monitoring has been running since the Program Start Time.
Nagios PID	Nagios Linux process identifier (PID).
Notifications Enabled?	If notifications are currently enabled, in general. Even if Yes, notifications can be disabled for individual hosts or services. If No, however, notifications are disabled for all hosts and services.
Service Checks Being Executed?	If PCC is currently monitoring services, in general. Even if Yes, individual service checks can be disabled. If No, however, <i>no</i> services are checked.
Running As A Daemon?	If monitoring process (Nagios) is running as a daemon. This is always Yes.
Last External Command Check	Time of latest execution of external command. See External Command Interface view, on page 2-143 . (When you submit a command, a short delay can elapse before the Control Center executes it.)

Table 2-48: Program Information chart, Nagios Info view (continued)

Variable	Description
Last Log File Rotation	<p>Time and date of latest event log file rotation. During daily rotation, file is copied from the log directory (/var/log/nagios) to the log archive directory (/var/log/nagios/archives).</p> <p>Log file is of limited size; when full, oldest log entries are discarded to make room for new entries. Log file is rotated daily to provide a record of past entries.</p>

Some Program Information chart variables appear in the Process Commands box as commands to change current values.



Process State Information chart

Table 2-49: Process State Information chart, Nagios Info view

Variable	Description
Process Status	<p>Status of monitoring process (Nagios). Should be OK. If not, use the command Restart the Nagios process. See Process Commands box, on page 2-69. Process status values are the same as service status values. See Host and service status values, on page 2-14.</p>

Process Commands box

Use the Process Commands box to run commands that perform actions. These actions are global, affecting all hosts and services. For example, if you disable notifications here, no notifications are sent for any hosts or services.

Commands with an adjacent X icon () or check-mark icon () are toggles. The icon indicates the new toggle state (after command execution): a check mark means enable or start; an X means disable or stop.

Click a command link to display the External Command Interface view for the command. See [External Command Interface view, on page 2-143](#).

Commands that disable (notifications, status checks, and so on) override commands that enable. For example, suppose you disable checks for a particular service, such as PING, using the Service Information view (command Disable checks of this service), but enable checks for all services using the Nagios Info view (command Start executing service checks). That particular service (PING) is *not* checked because disabling overrides enabling.

Related Views

- For information about commands affecting only specific host groups, hosts, and services, see [Hostgroup Information view, on page 2-121](#), [Host Information view, on page 2-126](#), and [Service Information view, on page 2-133](#).
- To disable notifications for a single host or service over a defined period, schedule downtime for it. See [Host Downtime view, on page 2-65](#).

Table 2-50: Links to Nagios Info view

Origin	Link
left menu	Nagios Info

Table 2-51: Links from Nagios Info view

Destination	Link
External Command Interface view, on page 2-143	command (see Process Commands box, on page 2-69 .)

Process Commands section

This section contains links to commands that perform actions on a specific host group. To execute a command:

1. Click on any link listed in Table 2-52. The External Command Interface view for that command appears. See [External Command Interface view, on page 2-143](#), for more information.
2. In the Command Options section, click Commit.

Table 2-52: Process commands, Nagios Info view

Command link	Description
Shutdown the Nagios process	Shuts down Nagios process. <i>Note:</i> After Nagios is shut down, it cannot be restarted via the web interface.
Restart the Nagios process	Restarts Nagios process. This is equivalent to sending the process a HUP signal. All information is flushed from memory, configuration files are reread, and Nagios starts monitoring with new configuration information.
Enable automatic email notifications for important system events	Enables host and service notifications on program-wide basis.
Stop executing service checks	Temporarily stops execution of service checks, and prevents notifications from being sent (for all services and hosts). Service checks are not executed again until you issue a command to resume service check execution.
Stop accepting passive service checks	Stops acceptance of passive service check results found in external command file. All passive check results found are ignored.
Disable event handlers	Temporarily stops host or service event handlers.
Start obsessing over services	Tells Nagios to start obsessing over service checks. Read the documentation on distributed monitoring for more information.
Enable flap detection	Enables flap detection for hosts and services on program-wide basis. Individual hosts and services might have flap detection disabled.
Disable failure prediction	Disables failure prediction for hosts and services on program-wide basis.
Disable performance data	Disables processing of performance data for hosts and services on program-wide basis.

Nagios Stats view

This view provides information about service monitoring performance. The gray-box heading for this view is Performance Information.

Table 2-53: Nagios Stats view features

Feature	Description
Time Frame/ Checks Completed	Number and percentage of PCC services checked in each indicated time frame (since PCC startup or in the last 1, 5, 15, or 60 minutes).
Metric/Min/Max/Average	Minimum, maximum, and average times:
• Check Execution Time	• it took to check a service
• Check Latency	• between time a service check was scheduled and time it was executed
	(Percent State Change is <i>not used</i> .)

The charts Passive Service Checks are *not used*; all PCC service checks are active.

Related Views

- [Hostgroup Information view, on page 2-121](#), presents the same monitoring performance information, but for a single host group (and you can execute host group commands).
- [Tactical Monitoring view, on page 2-50](#), also provides limited information about monitoring performance.

Table 2-54: Links to Nagios Stats view

Origin	Link
left menu	Nagios Stats
Tactical Monitoring view, on page 2-50	Monitoring Performance

Table 2-55: Links from Nagios Stats view

Destination	Link
Service Detail view, on page 2-53	Active Service Checks (<#> Total)

Scheduling Queue view

Use this view to display and schedule service checks. This view provides information about when each service on each host is scheduled to be checked. The gray-box heading for this view is **Service Check Scheduling Queue**.

Current sort order is indicated by the heading above the chart, for example, **Entries sorted by next check time (ascending)**. Some chart column headings have associated vertical arrows. To sort the chart in ascending order by a given column, click the orange up arrow. To sort in descending order, click the green down arrow. By default, charts are sorted by Next Check time in ascending order.

Table 2-56: Scheduling Queue view features

Feature	Description
Host	Hosts in system scheduled to be checked.
Service	Services scheduled to be checked.
Last Check	Time service was last checked.
Next Check	Time service is scheduled to be checked next.
Active Checks	Whether service is being monitored (ENABLED) or not (DISABLED). (All PCC checks are active, not passive, checks.)

Table 2-57: Links to Scheduling Queue view

Origin	Link
left menu	Scheduling Queue

Table 2-58: Links from Scheduling Queue view

Destination	Link
Host Information view, on page 2-126	host name
Service Information view, on page 2-133	service name
External Command Interface view, on page 2-143	Actions icon – see above



Displaying status information for specific hosts

In the Host column, click host name, such as sc-sc1-172-1. See [Host Information view, on page 2-126](#).


Displaying status information for specific services

In the Service column, click service name, such as PING. See [Service Information view, on page 2-133](#).

Disabling or enabling service checks

Click the X icon () or check-mark icon () to disable or enable service checks, respectively. The External Command Interface view appears, where you confirm enabling or disabling. See [External Command Interface view, on page 2-143](#).

Rescheduling services

Click the wristwatch icon () to reschedule service. The External Command Interface view appears. If you select the check box Force Check in the External Command Interface view, service is checked at newly scheduled time even if service is disabled at that time.

Reporting folder

Email Reporter view

Use this view to configure summary monitoring reports to be sent periodically to email recipients you choose. You choose report types to send and how often to send them.

For each report type (ReportTypes), Detailed and TextSummary, choose a reporting period (NotificationGroups) and any number of email recipients (Members). For example, you might make the following configuration choices:

- Send Detailed report `Once_A_Day` to `ddiderot@ncyclo.com` and `ghegel@yinyangquanta.org`
- Send TextSummary report `Every_Two_Hours` to `myself@myisp.com`
- Send TextSummary report `Every_Eight_Hours` to `mycolleague@isp.com`

Table 2-59: Email Reporter view features

Feature	Description
ReportTypes	<p>Currently configured email report types.</p> <p>Select report type:</p> <ul style="list-style-type: none">• Detailed: HTML report of host and service problems, smart cell information, performance graphs, and exceptions. See Detailed email reports, on page 2-77.• TextSummary: Plain-text ASCII report of domain-specific information such as storage size, host and service problems, and locations of exceptions. See Text summary email reports, on page 2-79. Suitable for mobile email devices. <p>If report type you want to configure is not yet listed, select it from the pull-down list, and click Add.</p> <p>To cancel all Detailed or TextSummary email reports, select type, and click Delete.</p>

Table 2-59: Email Reporter view features (continued)

Feature	Description
NotificationGroups	<p>Currently configured email report periods. Choose how often to send email report:</p> <ul style="list-style-type: none"> • Every_Two_Hours • Every_Four_Hours • Every_Six_Hours • Every_Eight_Hours • Every_Ten_Hours • Twice_A_Day • Once_A_Day <p>If the period you want is not listed, select it from the pull-down list, and click Add.</p> <p>To cancel all email reports scheduled for given period, select period, and click Delete.</p>
Members	<p>Recipient email addresses for report corresponding to selected ReportTypes and NotificationGroups fields.</p> <p>To add recipient, enter email address, and click Add.</p> <p>To remove recipient, select email address, and click Delete.</p>

See Also

- [Detailed email reports, on page 2-77](#), and [Text summary email reports, on page 2-79](#), for information about interpreting report emails.

Related Views

- [System Status view, on page 2-20](#), provides similar information to email reports.

Table 2-60: Links to Email Reporter view

Origin	Link
left menu	Email Reporter

Links **from** Email Reporter view: none

Detailed email reports

Detailed email reports provide system status and performance information in an HTML document. The detailed HTML format provides more content and the format is more sophisticated than the text summary report.

The following information is provided in detailed reports:

- Appliance Performance: Information available through the System Status view (see [System Status view, on page 2-20](#)).
 - For each domain: Number of messages stored, rate of messages stored, rate of messages replicated, and number of signatures stored (if backup is enabled).
 - For system (all domains): Total number of messages stored, average rate of messages stores, average rate of messages replicated, and number of signatures stored (if backup is enabled).
 - Number of messages in system **catch-all repository**, including messages too large to be indexed, messages that cannot be parsed, and messages that cannot be routed to a registered RISS user.

Messages that cannot be parsed have malformed message structures (MIME) or unsupported character sets.

Messages that cannot be routed do not correspond to any system routing rule. They are not recognized as destined for a registered RISS user. Mailing-list messages cannot be routed if the recipient name is not included in the message as a destination.

- Store Rate graph: Number of store operations per second, measured hourly over current day, starting at midnight. This graph is one of the Application Performance Info graphs available from the System Status view, Other Graphs link, with Display Type: Min/Max/Avg and Time Frame: Hours in a day.
- Host Problems: Subset of information in the Host Detail view, providing information only about hosts that have problems (see [Host Detail view, on page 2-56](#)).
- Service Problems: Subset of information in the Service Detail view, providing information only about services that have problems (see [Service Detail view, on page 2-53](#)).

- Smart Cell Metrics: Subset of the Smart Cell Groups for Domain view (see [Displaying the Smart Cell Groups for Domain view, on page 2-23](#)). For each domain, includes the following metrics for each smart cell in each smart cell group:
 - Role: If smart cell is primary, secondary, or first or second replica of smart cell group.
 - HostName: Smart cell's IP address.
 - State: Smart cell's current life cycle state. See [Smart cell life cycle states, on page 2-13](#).
 - NumArchived: Number of messages smart cell archived since it was assigned.
 - NumIndexed: Number of messages smart cell indexed since it was assigned.
 - NumFailedDocs: Number of messages smart cell did not index since system startup.
 - NumBackedUpDocs: Number of messages smart cell backed up since system startup (if backup option is installed).
 - Store Rate: Rate (per second) of storage operations on smart cell at time of report.
- Free Smart Cells: List of smart cells in free state at time of report.
- Domain Configuration: For each domain: set size (number of groups that can be created), disabled/enabled state of compliance, backup, replication, and replica count (number of replicas to be created for each group).
- Software Versions: Versions of RISS software currently installed, including:
 - Application: Third-party software package, also called L3.
 - Installer: Reference Information Storage System installation program.
 - Linux and Windows Cores: Reference Information Storage System and operating system software on Linux and Windows servers, also called L2 and W2, respectively.
 - Windows System: Windows software, also called W3.
- Installed Patches: Reference Information Storage System software patches installed.

In addition to information in the report itself, plain-text attachments provide exception logs for the following host groups:

- SmartCell_Exceptions.txt: Smart cells host group
- MetaServer_Exceptions.txt: Metaserver host group
- HTTP_Exceptions.txt: HTTP portals host group
- SMTP_Exceptions.txt: SMTP portals host group
- LogServer_Exceptions.txt: TSC-NAT host group

This is the same information available through the Exceptions field links in the System Status view. If no exceptions have occurred since respective servers started, there is no link and no log attached to the detail report. Any exceptions older than those in attachments were pruned from the event log when it filled up.

See Also

- [Text summary email reports, on page 2-79](#)
- [Host Problems view, on page 2-62](#)
- [Service Problems view, on page 2-61](#)
- [Displaying the Smart Cell Groups for Domain view, on page 2-23](#)
- [System Status view, on page 2-20](#)

Text summary email reports

Text summary email reports provide a short, plain-text summary of system status and performance information. The plain-text format creates a smaller message size than the detailed HTML report. You can access text summary reports from wireless handheld email devices.

The following information is provided in plain-text summary reports:

- Report identification: Date, time, and site name
- Versions of Reference Information Storage System software currently used: Spine (also called L2: foundation software, including operating systems), Application (also called L3), and Installer

- For each domain (DOMAIN SPECIFIC INFORMATION):
 - Domain name
 - Number of smart cell groups (SetSize)
 - If system is ready for storage operations (SMTP portals are ready and smart cells are allocated for domain)
 - If system is currently storing
 - If system is currently backing up data
 - If system is currently backing up message signatures
 - Size in gigabytes of raw data (documents) to be stored, before compression
 - Percentage of disk utilization
- Number of FREE smart cells, total number of smart cells, FREE/total ratio as a percentage
- Hosts currently having problems
- Services currently having CRITICAL problems (and their hosts)
- Host groups where exceptions are currently logged (same as Exceptions field links of System Status view – see [System Status view, on page 2-20](#))

See Also

- [Detailed email reports, on page 2-77](#)
- [System Status view, on page 2-20](#)

Creating or editing email report configurations

1. Check given report configuration, and select its entries in the ReportTypes and NotificationGroups fields. Report recipients are listed in the Members field.
2. Select NotificationGroups or Members as needed.
3. Click Submit Configuration.

Editing reports

1. In the Report Types list, select report. Email report periods appear in the Notification Groups list.
2. Select email report period. Recipients appear in the Members list.
3. To edit the Members list, add email address and click Add, or select email address and click Delete.
4. Click Submit Configuration.

LogFile Sender view

The LogFile Sender view allows you to select log files to send to HP to assist in troubleshooting. This feature exists as an alternative to using the command line prompt to send log files.

Trends view

Use this view to create reports on status of individual hosts or services over given time periods.

Table 2-61: Trends view features

Feature	Description
heading	<ul style="list-style-type: none">• Name of host or service reported on.• Covered report period.

Table 2-61: Trends view features (continued)

Feature	Description
State History	<p>Color-coded chart indicating host/service status value trends over reported time period.</p> <div></div> <p>Pause the mouse pointer over status bar to display tooltip of additional information. (Pausing has no effect if Suppress pop-ups is turned <i>on</i> – see Creating trends reports, on page 2-84.)</p> <p>Example tooltip:</p> <div><p>DOWN</p><p>Time Range: <i>Fri Dec 6 09:10:49 2002 to Fri Dec 6 09:14:21 2002</i></p><p>Duration: <i>0d 0h 3m 32s</i></p><p>State Info: <i>CRITICAL - Plugin timed out after 10 seconds</i></p></div> <p>Click status color in the Status History chart to zoom in by the Zoom factor (see below). (Clicking has no effect if Suppress image map is turned <i>on</i> – see Creating trends reports, on page 2-84.)</p>
State Breakdowns	<p>Summary chart showing total elapsed time for each host or service status value since PCC monitoring startup (in parentheses, expressed as percentage of total time).</p>

The same color coding is used in both charts: State History and State Breakdowns. See [Host and service status values, on page 2-14](#) for more information. The additional value Indeterminate used in these charts generally indicates time the entire system (site) was not operational.

In addition to report features described previously, the report view has an input form at the upper right you can use to update the report. After changing report options, click **Update** to regenerate the report with new options.

Input form options you can set are the same as those used to create displayed report: Assume initial states, Report period, and so on, with the addition of the Zoom factor. The Zoom factor affects how much each mouse click zooms into the Status History chart (see State History feature, above). A larger factor zooms more.

Related Views

- [Availability view, on page 2-85](#), lets you create a report on availability of individual hosts, services, or host groups over given time periods.
- [Alerts History view, on page 2-97](#), shows logged alerts.
- [Creating availability reports, on page 2-88](#), shows number of alerts of different types for hosts and/or services.

Table 2-62: Links to Trends view

Origin	Link
left menu	Trends
Availability view, on page 2-85 , for single host or service	<ul style="list-style-type: none"> • View Trends For This Host/Service • status bar chart
Creating availability reports, on page 2-88	View Trends For This Host/Service
Alerts History view, on page 2-97 , for single host or service	View Trends For This Host/Service
Notifications view, on page 2-89 , for single host or service	View Trends For This Host/Service
Host Information view, on page 2-126	View Trends For This Host
Service Information view, on page 2-133	View Trends For This Service
Trends view of service	View Trends For This Host

Table 2-63: Links from Trends view

Destination	Link
Trends view for host this service is running on (when view shows <i>service</i> trends)	View Trends For This Host
Availability view, on page 2-85 , for host or service	View Availability Report For This Host/Service
Creating availability reports, on page 2-88 , for host or service	View Alert Histogram For This Host/Service
Service Detail view, on page 2-53 , for host (when view shows <i>host</i> trends)	View Status Detail For This Host
Alerts History view, on page 2-97 , for host or service	View Alert History For This Host/Service
Notifications view, on page 2-89 , for host or service	View Notifications For This Host/Service

Creating trends reports

1. Choose report type: Host or Service.
2. Choose host or service.
3. Choose report options. You typically choose the Report Period (first option) and use defaults for other options.
 - Report Period: Choose predefined period (Last 24 Hours, Today, Yesterday, This Week, Last 7 Days, Last Week, This Month, Last Month, This Year, Last Year); or choose * CUSTOM REPORT PERIOD *, and specify custom report start and end dates.
 - Assume Initial States: Choose Yes to assume any undetermined status value is really the First Assumed State. Choosing No is equivalent to choosing Yes, and choosing Unspecified as the First Assumed State.
 - Assume State Retention: Choose Yes to use last recorded status value before PCC startup as status value assumed for periods when monitoring was down.
 - First Assumed State: Choose status value assumed for periods when monitoring was down. Has no effect if Assume Initial States is No or Assume State Retention is Yes.

- Backtracked Archives: *Not used*
- Suppress image map: Turn on to inhibit zooming into the State History chart by clicking status color.
- Suppress popups: Turn on to inhibit display of tooltips in State History chart status bars.

4. Click Create Report.

Availability view

Use this view to create reports on availability of individual hosts, services, or host groups, over given time periods.

Table 2-64: Availability view features, single host or service


Feature	Description
heading	<ul style="list-style-type: none"> • Name of host or service reported on. • Covered report period.
Host/Service State Breakdowns	<p>Color-coded history chart indicating host/service status value trends over reported time period. This is a reduced version of the corresponding Trends view.</p>  <p>Click bar chart to display the full Trends view. See Alerts folder, on page 2-94.</p> <p>For each host or service status value and each Type/Reason, chart indicating:</p> <ul style="list-style-type: none"> • Time: Duration of status value. • % Total Time: Duration of status value, as percentage of total time since PCC monitoring started. • % Known Time: Duration of status value, as percentage of total time since PCC monitoring started minus time with Undetermined status. <p>Each determined status value is divided into Scheduled and Unscheduled periods, depending on if downtime was scheduled. Status can be Undetermined because monitoring was not running at the time, or because not enough data was available to determine status value.</p>

Table 2-64: Availability view features, single host or service (continued)

Feature	Description
State Breakdowns For Host Services (host report only)	For each service running on host, percent of total elapsed time for each service status value. Values in parentheses represent percentages of total time minus time with Undetermined status. Click service name to view service Availability report.
Host/Service Log Entries	For each host/service event, event start and end time, duration, type, and descriptive information. Click link to toggle between viewing only problem events (condensed log entries) and all logged events (full log entries).

Table 2-65: Availability view features, single host group, or all host groups, hosts, or services

Feature	Description
heading	<ul style="list-style-type: none"> Name of report: Individual host group, All Hostgroups, Hosts, or Services. Covered report period.
Host/Service State Breakdowns For host group reports, Host State Breakdowns are organized by host group.	For each host or service, and each of its status values: <ul style="list-style-type: none"> % Time <status value>: Duration of status value, as percentage of total time and, in parentheses, as percentage of total time minus time with Undetermined status.

In addition to report features described previously, each report view has an input form at the upper right you can use to update the report using different options. Options you can set are the same as those used to create displayed report: Assume initial states, Report period, and so on. After changing report options, click Update to regenerate the report with new options.

Table 2-66: Links to Availability view

Origin	Link
left menu	Availability

Table 2-66: Links to Availability view (continued)

Origin	Link
Alerts folder, on page 2-94	View Availability Report For This Host/Service
Creating availability reports, on page 2-88	View Availability Report For This Host/Service
Hostgroup Information view, on page 2-121	View Availability Report For This Hostgroup
Host Information view, on page 2-126	View Availability Report For This Host
Service Information view, on page 2-133	View Availability Report For This Service
Availability report for single host or service	View Availability Report For All Hosts/Services
Availability report for single service	View Availability Report For This Host
Availability report for single host	service name

All links from the Availability view use the same report options for destination view as were used for current availability report.

Table 2-67: Links from Availability view

Destination	Link
From <i>single</i> host report	
Availability report for single service	service name
From <i>single</i> host or service report	
Availability report for <i>all</i> hosts/services	View Availability Report For All Hosts/Services
Alerts folder, on page 2-94 , for host or service	View Trends For This Host/Service
Creating availability reports, on page 2-88 , for host or service	View Alert Histogram For This Host/Service
Alerts History view, on page 2-97 , for host or service	View Alert History For This Host/Service
Notifications view, on page 2-89 , for host or service	View Notifications For This Host/Service

Table 2-67: Links from Availability view (continued)

Destination	Link
From <i>single host</i> report	
Service Detail view, on page 2-53 , for host	View Status Detail For This Host
From <i>single service</i> report	
Availability report for host this service is running on	View Availability Report For This Host

Creating availability reports

1. Choose report type: Hostgroup(s), Host(s), or Service(s).
2. Depending on report type, choose host group, host, or service; or choose all host groups, hosts, or services.
3. Choose report options. You typically choose the Report Period (first option) and use defaults for other options.
 - Report Period: Choose predefined period (Last 24 Hours, Today, Yesterday, This Week, Last 7 Days, Last Week, This Month, Last Month, This Year, Last Year); or choose * CUSTOM REPORT PERIOD *, and specify custom report start and end dates.
 - Assume Initial States: Choose Yes to assume any undetermined status value is really the First Assumed State. Choosing No is equivalent to choosing Yes, and choosing Unspecified as the First Assumed State.
 - Assume State Retention: Choose Yes to use last recorded status value before PCC startup as status value assumed for periods when monitoring was down.
 - First Assumed State: Choose status value assumed for periods when monitoring was down. Has no effect if Assume Initial States is No or Assume State Retention is Yes.
 - Backtracked Archives: *Not used*
 - Select the check box Output in CSV Format if you want the report in comma-separated value format instead of HTML. Available only for reports on all hosts or services. This is useful if you need to insert the generated report into a spreadsheet.

4. Click Create Availability Report.

Notifications view

This view provides a chronology of host and service notifications sent to system contact. It shows notifications for specific host, specific service, or all hosts and services, depending on how the view is accessed.

Notifications are sent whenever host or service problems are detected or resolved. You can filter this view to display only specific notification types, and display notifications for any given day.

Note: Notifications are logged only if Notifications have been enabled.

Table 2-68: Notifications view features

Feature	Description
Log File Navigation	Day covered by current view.
	Click left (right) arrow to view notifications from previous (next) day.
Host	Origin of notification (corresponds to the Host field of notification email).
	Click link for details. See Host Information view, on page 2-126 .
Service	Origin of notification (corresponds to the Service field of notification email). Service is N/A (not available) if host is down.
	Click link for details. See Service Information view, on page 2-133 .
Type	Notification type, color coded (corresponds to the Notification Type field of notification email). Blue: information, green: normal, yellow: warning, red: failure, orange: unknown. Examples: HOST DOWN, CRITICAL, ACKNOWLEDGEMENT
Time	Date and time notification was sent (corresponds to the Date/Time field of notification email).
Contact	Notification contact name: administrator account, admin
	Click the admin contact link for details. See Contacts in View Config view, on page 2-107 .

Table 2-68: Notifications view features (continued)

Feature	Description
Notification Command	Notification command name (defined during system configuration). Click link for details. See Commands in View Config view, on page 2-107 .
Information	Additional information (corresponds to the Additional Info field of notification email)
update form (upper right)	To update the Notifications view: 1.Choose the following update options: – To show only certain types of notification, choose notification type in the pull-down list Notification detail level. – To change notification list order, click the check box Older Entries First. 2.Click Update.

See Also

- [View Config view, on page 2-107](#), for object types Hosts, Services, and Contacts; describes host and service status values causing notifications to be sent.

Related Views

- Information in the Notifications view is a subset of that in the Event Log view. See [Event Log view, on page 2-92](#).

Table 2-69: Links to Notifications view

Origin	Link
left menu	Notification
Service Detail view, on page 2-53 , when main heading is Service Status Details For All Hosts	View Notifications For All Hosts
Service Problems view, on page 2-61	View Notifications For All Hosts

Table 2-69: Links to Notifications view (continued)

Origin	Link
Alerts History view, on page 2-97 <ul style="list-style-type: none"> • for all hosts and services • single host • single service 	View Notifications For: <ul style="list-style-type: none"> • All Hosts • This Host • This Service
Alerts folder, on page 2-94	View Notifications For This Host/Service
Availability view, on page 2-85 , for single host or service	View Notifications For This Host/Service
Creating availability reports, on page 2-88	View Notifications For This Host/Service
Host Information view, on page 2-126	View Notifications For This Host
Service Information view, on page 2-133	View Notifications For This Service

Table 2-70: Links from Notifications view

Destination	Link
When main view heading is All Hosts and Services	
Service Detail view, on page 2-53	View Status Detail For All Hosts
Alerts History view, on page 2-97	View History For All Hosts
When view shows notifications for single host or service	
Alerts History view, on page 2-97 , for host/service	View History For This Host/Service
Alerts folder, on page 2-94 , for host/service	View Trends For This Host/Service
When view shows notifications for single host	
Service Detail view, on page 2-53 , for host	View Status Detail For This Host
When main view heading is All Contacts and view shows notifications	
Host Information view, on page 2-126	specific host name
Service Information view, on page 2-133	specific service name

Event Log view

This view provides a chronology of logged PCC events.

The Nagios event log (file `/var/log/nagios/nagios.log`) is rotated daily at midnight, and a copy named with the date (for example, `nagios-12-20-2002-00.log`) is placed in the archive directory, `/var/log/nagios/archives`.

Table 2-71: Event Log view features

Feature	Description
update form (upper right)	To update the Event Log view to change event list order, click the check box Older Entries First, and click Update.
Log File Navigation	Day covered by current view.
	Click left (right) arrow to view events from previous (next) day.
events	<div>Information for event, including (not all event types include all information):</div> <ul style="list-style-type: none">• Color-coded status icon (blue: information, green: normal, yellow: warning, red: failure, orange: unknown).• Time stamp.• Event type: HOST or SERVICE.• Host identifier.• Service identifier (service alerts only).• Host or service status value. See Host and service status values, on page 2-14.• Status condition (HARD or SOFT). See Hard and soft status conditions, on page 2-15.• Sequential identifier for this event message. Indicates how many times it has been sent.• Event message: additional information describing event.

Related Views

- The information in the Alert History view is a subset of that in the Event Log view. See [Alerts History view, on page 2-97](#).
- [Creating availability reports, on page 2-88](#), shows number of alerts of different types for hosts and/or services.

- [Alerts folder, on page 2-94](#), shows status value trends over time for hosts and/or services.

Table 2-72: Links **to** Event Log view

Origin	Link
left menu	Event Log

Links **from** Event Log view: none

Alerts folder

Alerts Histogram view

Use this view to create reports with simple graphs showing, for individual hosts or services, number of events of different types over different time periods.

The following histogram shows all service events over a one-day period. It shows, for example, two CRITICAL events and three WARNING events occurred around 6:45, and two recovery (OK) events occurred around 7:00.

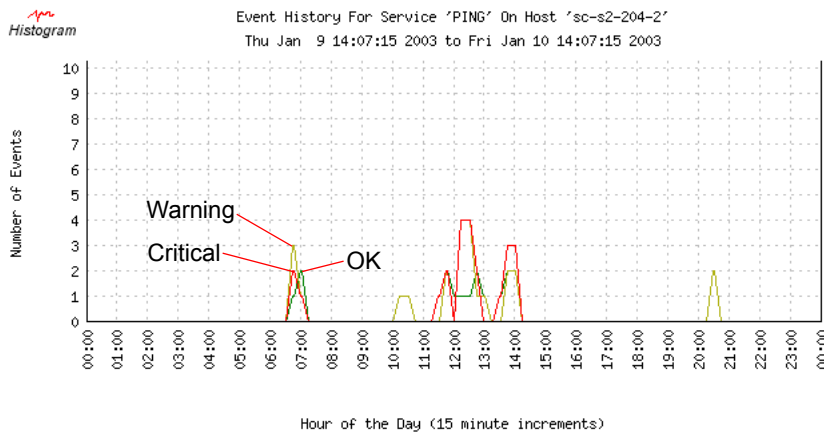


Figure 2-2: Alerts histogram of all service events over one-day period

Whenever graph lines for events of different status values overlap exactly, only the most severe status value is indicated. To see an event line that is hidden by overlapping, create a separate histogram for just the hidden status

value. For example, the following histogram shows only recovery (OK) events for the same time period. The OK event line from 11:15 to 13:15 was hidden by CRITICAL and WARNING event lines in the previous histogram.

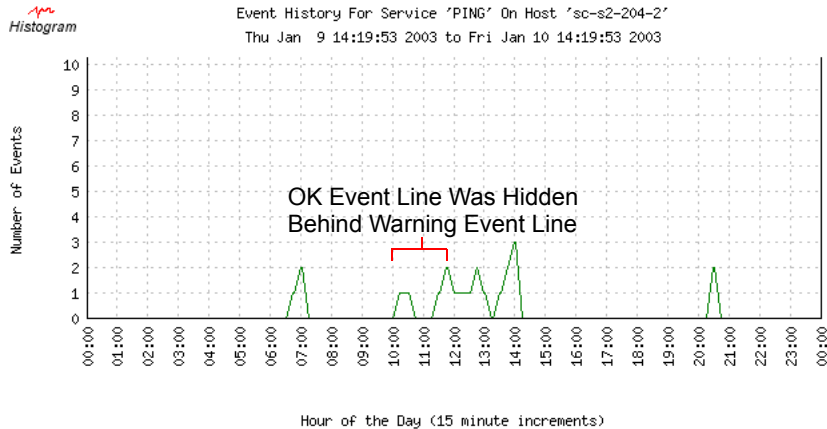


Figure 2-3: Alerts histogram of recovery service events over one-day period

Table 2-73: Alerts Histogram view features

Feature	Description
heading	<ul style="list-style-type: none"> Name of host or service reported on. Covered report period.
Event History	Color-coded graph indicating host/service event history over reported time period. See Host and service status values, on page 2-14 , for information about color coding of status values.
event breakdowns	Summary chart showing number of events associated with each host/service status value over covered time period. Minimum, maximum, total, and average number of events are reported. The same status value colors are used as in the Event History graph.

The same status colors are used in both charts: graph and event breakdowns. See [Host and service status values, on page 2-14](#), for descriptions of possible status values.

In addition to report features described previously, the report view has an input form at the upper right you can use to update the report. After changing report options, click **Update** to regenerate the report with new options. Input form options you can set are the same as those used to create the displayed report: Report period, Assume state retention, and so on.

Related Views

- [Alerts folder, on page 2-94](#), shows status value trends for hosts or services.
- [Alerts History view, on page 2-97](#), shows detailed chronology of events for hosts and/or services.

Table 2-74: Links to Alerts Histogram view

Origin	Link
left menu	Alerts Histogram
Alerts folder, on page 2-94 , for specific host or service	View Alert Histogram For This Host/Service
Availability view, on page 2-85 , for specific host or service	View Alert Histogram For This Host/Service
Host Information view, on page 2-126 , for specific host	View Alert Histogram For This Host
Service Information view, on page 2-133 , for specific service	View Alert Histogram For This Service

Table 2-75: Links from Alerts Histogram view

Destination	Link
Alerts folder, on page 2-94 , for host or service	View Trends For This Host/Service
Availability view, on page 2-85 , for host or service	View Availability Report For This Host/Service
Alerts History view, on page 2-97 , for host or service	View History For This Host/Service
Notifications view, on page 2-89 , for host or service	View Notifications For This Host/Service

Table 2-75: Links from Alerts Histogram view (continued)

Destination	Link
Service Detail view, on page 2-53 , for host	View Status Detail For This Host

Creating alert histogram reports

1. Choose report type: Host or Service.
2. Choose host or service.
3. Choose report options:
 - Report Period: Choose predefined period (Last 24 Hours, Today, Yesterday, This Week, Last 7 Days, Last Week, This Month, Last Month, This Year, Last Year); or choose * CUSTOM REPORT PERIOD *, and specify custom report start and end dates.
 - Statistics Breakdown: Choose time scale to use for Report Period: Month, Day of the Month, Day of the Week, or Hour of the Day.
 - Events To Graph: Choose type of host or service events to report on: events indicating change to specific status value, all problem status values, or all events.
 - State Types To Graph: Choose status conditions to graph: HARD, SOFT, or both. See [Hard and soft status conditions, on page 2-15](#).
 - Assume State Retention: Typically, you use the default, Yes. Choose Yes to use last recorded status value before PCC startup as status value assumed for periods when monitoring was down.
 - Initial States Logged: *Not used*
 - Ignore Repeated States: *Not used*
4. Click Create Report.

Alerts History view

This view provides a chronology of logged PCC alerts. Alerts are a subset of events listed in the Event Log view. You can filter this view to display only specific alert types, and display alerts for any given day.

Table 2-76: Alerts History view features

Feature	Description
Log File Navigation	Day covered by current view. Click left (right) arrow to view alerts from previous (next) day.
alerts	Information for each alert, including: <ul style="list-style-type: none"> • Color-coded status icon (green: normal, yellow: warning, red: failure, orange: unknown). • Time stamp. • Alert type: HOST or SERVICE. • Host identifier. • Service identifier (service alerts only). • Host or service status value. See Host and service status values, on page 2-14. • Status condition (HARD or SOFT). See Hard and soft status conditions, on page 2-15. • Sequential identifier for alert message. Indicates how many times it has been sent. • Alert message (additional information describing alert).
update form (upper right)	• Updates the Alerts History view.

Related Views

- The information in the Alerts History view is a subset of that in Event Log view. See [Event Log view, on page 2-92](#).
- [Creating availability reports, on page 2-88](#), shows number of alerts of different types for hosts and/or services.
- [Alerts folder, on page 2-94](#), shows status value trends for hosts and/or services.

Table 2-77: Links to Alerts History view

Origin	Link
left menu	Alerts History

Table 2-77: Links to Alerts History view (continued)

Origin	Link
Service Detail view, on page 2-53 , when main heading is Service Status Details For All Hosts	View History For All Hosts
Service Problems view, on page 2-61	View History For All Hosts
Notifications view, on page 2-89 <ul style="list-style-type: none"> • when gray-box heading is Notifications • single host • single service 	View History For: <ul style="list-style-type: none"> • All Hosts • This Host • This Service
Host Information view, on page 2-126	View Alert History For This Host
Service Information view, on page 2-133	View Alert History For This Service
Alerts folder, on page 2-94	View History For This Host/Service
Availability view, on page 2-85 , for single host or service	View History For This Host/Service
Creating availability reports, on page 2-88	View History For This Host/Service
Alert History, for single service	View History For This Host

Table 2-78: Links from Alerts History view

Destination	Link
When view shows alerts for all hosts and services	
Service Detail view, on page 2-53	View Status Detail For All Hosts
Notifications view, on page 2-89	View Notifications For All Hosts
When view shows alerts for single host or service	
Notifications view, on page 2-89 , filtered for host/service	View Notifications For This Host/Service
Alerts folder, on page 2-94 , filtered for host/service	View Trends For This Host/Service
When view shows alerts for single host	
Service Detail view, on page 2-53 , filtered for host	View Status Detail For This Host

Table 2-78: Links from Alerts History view (continued)

Destination	Link
When view shows alerts for single service	
Alert History view, filtered for host where service is running	View History For This Host

Updating Alerts History view

- Choose the following update options:
 - To show only alerts about certain status conditions, choose a condition (SOFT, HARD, All) from the State type options list. See [Hard and soft status conditions, on page 2-15](#).
 - To show only certain types of alerts, choose alert type from the History detail level list. For example, choose Service critical to show only alerts for services with status value CRITICAL.
 - To hide certain types of alerts, click the appropriate Hide check box.
 - To change alert list order, click the Older Entries First check box.
- Click Update.

Alerts Summary view

Use this view to create reports summarizing different types of alerts over different time periods. You can create several standard alert summary reports, or create custom alert summary reports.

Table 2-79: Alerts Summary view features, general

Feature	Description
heading	Choice made for Report Type and time period covered.
Report Options Summary	Other report creation options chosen. Click Generate New Report to change report options and create an Alert Summary report.

Table 2-79: Alerts Summary view features, general (continued)

Feature	Description
main chart heading	Brief description of report contents. Examples: <ul style="list-style-type: none"> • Displaying most recent 25 of 742 total matching alerts • Totals By Hostgroup
See Table 2-80, Table 2-81, and Table 2-82 for more information about specific report type features.	

Table 2-80: Alerts Summary view features, most recent alerts

Feature	Description
Time	Time of alert.
Alert Type	Host or service alert.
Host	Name of host. Click host name to display the Host Information view. See Host Information view, on page 2-126 .
Service	Name of service. Click service name to display the Service Information view. See Service Information view, on page 2-133 .
State	Host/service status value.
State Type	If status condition is HARD or SOFT. See Hard and soft status conditions, on page 2-15 .
Information	Alert message.

Note: For Alerts Summary reports of type Alert Totals (including those organized by host group, host, and service), totals are given for each possible host or service status value.

Table 2-81: Alerts Summary view features, alert totals

Feature	Description
State	Host/service status value. The row All States provides totals of each type of alert for all possible status values.
Soft Alerts	Number of SOFT alerts for given status value. See Hard and soft status conditions, on page 2-15 .
Hard Alerts	Number of HARD alerts for given status value.
Total Alerts	Total number of alerts (SOFT and HARD) for given status value.

Table 2-82: Alerts Summary view features, top alert producers

Feature	Description
Rank	Higher rank is indicated by smaller number, and means more alerts produced.
Producer Type	Host or service alert.
Host	Name of host. Click host name to display the Host Information view. See Host Information view, on page 2-126 .
Service	Name of service. Click service name to display the Service Information view. See Service Information view, on page 2-133 .
Total Alerts	Number of alerts produced by alert producer.

Table 2-83: Links to Alerts Summary view

Origin	Link
left menu	Alerts Summary

Table 2-84: Links from Alerts Summary view

Destination	Link
Host Information view, on page 2-126	host
Service Information view, on page 2-133	service

Creating standard alert summary reports

1. Choose standard Report Type under Standard Reports. Only alerts with HARD status conditions are reported. See [Hard and soft status conditions, on page 2-15](#).

Table 2-85: Standard alert summary report types

Standard report type	Information reported
25 Most Recent Hard Alerts	The 25 most recent HARD host and service alerts. Same as custom report of type Most Recent Alert (see Alerts Summary view features, most recent alerts, on page 2-101), except only HARD alerts are reported.
25 Most Recent Hard Host Alerts	Same as previous, but only HARD <i>host</i> alerts are reported.
25 Most Recent Hard Service Alerts	Same as previous, but only HARD <i>service</i> alerts are reported.
Top 25 Hard Host Alert Producers	The 25 hosts producing the most HARD alerts, ranked in order of number of alerts produced. Similar to custom report of type Top Alert Producers (see Alerts Summary view features, top alert producers, on page 2-102).
Top 25 Hard Service Alert Producers	Same as previous, but reports on services producing HARD alerts.

2. Click Create Summary Report (under Standard Reports).

Creating custom alert summary reports

1. Choose custom Report Type under Custom Report Options.

Table 2-86: Custom alert summary report types

Custom report type	Information reported
Most Recent Alerts	The 25 most recent alerts, with such details as alert time and alert message.
Alert Totals	Summary information about number of alerts for each host and service status value.
Alert Totals By Hostgroup	Same as Alert Totals, but totals for each host group.
Alert Totals By Host	Same as Alert Totals, but totals for each host.
Alert Totals By Service	Same as Alert Totals, but totals for each service.
Top Alert Producers	The 25 hosts and/or services producing the most alerts, ranked by number of alerts produced.

2. Choose report options:

- Report Period: Choose predefined period (Last 24 Hours, Today, Yesterday, This Week, Last 7 Days, Last Week, This Month, Last Month, This Year, Last Year); or choose * CUSTOM REPORT PERIOD *, and specify custom report start and end dates.
- Limit To Hostgroup: Choose host group to report on, or ** ALL HOSTGROUPS **.
- Limit To Host: Choose host to report on, or ** ALL HOSTS **.
- Alert Types: Choose to report on host alerts, service alerts, or both.
- State Types: Choose to report on alerts about HARD, SOFT, or both status conditions. See [Hard and soft status conditions](#), on page 2-15.
- Host States: Choose host status values to report on: UP, DOWN, UNREACHABLE, problem status values (DOWN, UNREACHABLE), or all host status values.
- Service States: Choose service status values to report on: OK, WARNING, UNKNOWN, CRITICAL, problem status values (WARNING, CRITICAL), or all service status values.

- Max List Items: Enter maximum number of alerts to report.
3. Click Create Summary Report.

Software Version view

This view shows software versions of hosts in each host group.

Table 2-87: Software Version view features

Feature	Description
Host Name	Host’s IP address. (Not available for HostType System.)
Spine Version	Reference Information Storage System software versions used. This software includes operating system.
Application Version	Reference Information Storage System software versions used.
Installer Version	Software versions used to install system.
Patches Applied	History of patches applied to system.

Table 2-88: Links to Smartcell Cloning view

Origin	Link
left menu	Software Versions

Links from Software Versions view: none

Viewing software versions on the system

You choose the host group using the HostType list. Alternatively, choose System as HostType to display all software versions of machines in the system. After selecting a HostType, click Update.

Displaying the patch history

Scroll down past the System Table section.

View Config view

This view shows system configuration from different viewpoints, based on different object types. You can examine *system parameters* as defined when system was configured. You *cannot change* any parameters; they are read-only.

This view always shows RISS settings made at system configuration/installation. This means that even though you can dynamically change some parameters displayed in the View Config view using other PCC views (for example, enabling/disabling host checking), the View Config values do *not* reflect these changes.

You choose the object type to display using the Object Type pull-down list at the upper right.

Table 2-89: View Config view features, hosts

Feature	Description
Host Name	Host's name. Example: sc-s2-204-4.
Alias/ Description	Host's long name or description. Example: SmartCellMachines:sc-s2-204-4.ourcompany.com.
Address	Host's IP address. Example: 10.0.204.4.
Parent Hosts	Host's parents. Example: cr-s0-96-4, cr-s0-96-3. <i>Note:</i> The only RISS hosts that have parent hosts are HTTP portals and smart cells (cloud routers are their parents).
Notification Interval	This is always No Renotification, meaning only one notification is sent when a host is detected as having a problem (see next).
Notification Options	Host status values that can cause notifications to be sent: DOWN, UNREACHABLE, and RECOVERY, where RECOVERY represents a transition from a problem status value (DOWN or UNREACHABLE) to the normal status value (UP).
Notification Period	Name of defined notification period: <i>always</i> , which means notifications can be sent any time; they are sent immediately. Click link to display definition of the <i>always</i> period. See View Config view features, time periods, on page 2-111 .

Table 2-89: View Config view features, hosts (continued)

Feature	Description
Max. Check Attempts	Maximum number of times to check host before a host problem status condition is considered HARD. See Hard and soft status conditions, on page 2-15 .
Host Check Command	Command used to check host. Click link to display command definition. See View Config view features, commands, on page 2-112 .
Enable Checks	If host checking is currently enabled.
Retention Options	Types of information retained in retention file, /usr/local/nagios/var/status.sav: all types of information.
(Not used by PCC: Event Handler, Enable Event Handler, Stalking Options, Enable Flap Detection, Low Flap Threshold, High Flap Threshold, Process Performance Data, Enable Failure Prediction, and Failure Prediction Options.)	

Table 2-90: View Config view features, host groups

Feature	Description
Group Name	Host group's name. Example: sc.
Description	Host group's description. Example: SmartCellMachines:sc-s2-204-4.ourcompany.com.
Default Contact Groups	Contact groups defined for host group: allAdmins is only contact group PCC uses. Click contact group link to display definition of contact group. See View Config view features, contact groups, on page 2-111 .
Host Members	All hosts in host group. Click host link to display configuration information for host. See View Config view features, hosts, on page 2-107 .

Table 2-91: View Config view features, services

Feature	Description
Host	<p>Name of host on which service is running.</p> <p>Click link to display configuration information for host. See View Config view features, hosts, on page 2-107.</p>
Description	Description of service. Example: Spine Check.
Max. Check Attempts	Maximum number of times to check service before a service problem status condition is considered HARD. See Hard and soft status conditions, on page 2-15 .
Normal Check Interval	Time between ordinary checks of service.
Retry Check Interval	Time between checks of service when it is not responding.
Check Command	<p>Command used to check service.</p> <p>Click link to display command definition. See View Config view features, commands, on page 2-112.</p>
Check Period	<p>Name of defined checking period: always, which means service can be checked any time.</p> <p>Click link to display definition of the always period. See View Config view features, time periods, on page 2-111.</p>
Enable Active Checks	If active service checks are currently enabled.
Default Contact Groups	<p>Contact groups defined for service: allAdmins is only contact group PCC uses.</p> <p>Click contact group link to display definition of contact group. See View Config view features, contact groups, on page 2-111.</p>
Enable Notifications	If notifications are currently enabled for service.
Notification Interval	This is always No Renotification, meaning only one notification is sent when a service is detected as having a problem (see next).
Notification Options	Service status values that can cause notifications to be sent: CRITICAL and RECOVERY, where RECOVERY represents a transition from a CRITICAL status value to the normal status value (OK).

Table 2-91: View Config view features, services (continued)

Feature	Description
Notification Period	Name of defined notification period: always , which means notifications can be sent any time; they are sent immediately. Click link to display definition of the always period. See View Config view features, time periods, on page 2-111 .
Retention Options	Types of information retained in retention file, <code>/usr/local/nagios/var/status.sav</code> : all types of information. (<i>Not used</i> by PCC: Parallelize, Volatile, Obsess Over, Enable Passive Checks, Check Freshness, Freshness Threshold, Event Handler, Enable Event Handler, Stalking Options, Enable Flap Detection, Low Flap Threshold, High Flap Threshold, Process Performance Data, Enable Failure Prediction, and Failure Prediction Options.)

Table 2-92: View Config view features, contacts

Feature	Description
Contact Name	Contact's name: admin is only contact PCC uses.
Alias	Contact's long name: Administrator .
Email Address	Contact's email address: bogus@persistcorp.com . Defined for the system at configuration time. <i>Note:</i> This can be a comma-separated list of email addresses. In that case, what is defined as contact (a single contact, <i>not</i> a contact group – see View Config view features, contact groups, on page 2-111) represents more than one email destination. Click link to compose and mail new message to contact.
Pager Address/Number	<i>Not used</i> by PCC.
Service Notification Options	Service status values that cause notifications to be sent to contact: CRITICAL and RECOVERY , where RECOVERY represents a transition from a CRITICAL status value to the normal status value (OK).
Host Notification Options	Host status values that cause notifications to be sent to contact: DOWN , and RECOVERY , where RECOVERY represents a transition from a problem status value (DOWN or UNREACHABLE) to the normal status value (UP).

Table 2-92: View Config view features, contacts (continued)

Feature	Description
Service Notification Period	<p>Name of defined notification period: always, which means notifications can be sent any time; they are sent immediately.</p> <p>Click link to display definition of the always period. See View Config view features, time periods, on page 2-111.</p>
Host Notification Period	<p>Name of defined notification period: always, which means notifications can be sent any time; they are sent immediately.</p> <p>Click link to display definition of the always period. See View Config view features, time periods, on page 2-111.</p>
Service Notification Commands	<p>Names of defined notification commands for services.</p> <p>Click link to display definition of command. See View Config view features, commands, on page 2-112.</p>
Host Notification Commands	<p>Names of defined notification commands for hosts.</p> <p>Click link to display definition of command. See View Config view features, commands, on page 2-112.</p>

Table 2-93: View Config view features, contact groups

Feature	Description
Group Name	Contact group's name: allAdmins is only contact group PCC uses.
Description	Contact group's description: All system administrators .
Contact Members	<p>Names of all contacts in contact group: admin is only contact PCC uses.</p> <p>Click the admin contact link to display definition of contact. See View Config view features, contacts, on page 2-110.</p>

Table 2-94: View Config view features, time periods

Feature	Description
Name	Name of defined time period: always .
Alias/Description	Long name or description of time period: alwaysContactMe .

Table 2-94: View Config view features, time periods (continued)

Feature	Description
< <i>day of week</i> > Time Ranges	Time period defined for given day of the week. The always time period has no time restriction on any day of the week.

Table 2-95: View Config view features, commands

Feature	Description
Command Name	Command's name. Example: check_ping.
Command Line	Command itself (its definition). Example: \$USER1\$/check_ping -H \$HOSTADDRESS\$ -w 200.0,20% -c 1000.0,60% -p 5.

Table 2-96: Links to View Config view

Origin	Link
left menu	View Config
Notifications view, on page 2-89	<ul style="list-style-type: none"> • admin contact (Contacts display) • specific command (Commands display)

Links **from** View Config view: none

Services tools folder

View Cell Space view

Use this view to determine data-archiving system status by providing information about hosts involved directly with the active-archive application. Also use this view to restore data when both smart cells in a group have failed.

To access this view, click View Cell Space in the left menu.

Note: This view is available only for system installers and advanced system administrators.

Table 2-97: View Cell Space view features

Feature	Description
<ul style="list-style-type: none"> • SMTP Portals • HTTP Portals • MetaServer • TSC-NAT 	Names of hosts in these host groups.
domains	<p>Smart cells of each domain, organized by smart cell group. Information about each smart cell group:</p> <ul style="list-style-type: none"> • Unique smart cell group identification number (RISS automatically generates ID). • Host names of smart cells in smart cell group, prefixed by P- (primary cell), S- (secondary cell), or R- (replication cell). • Each smart cell's life cycle state. See Smart cell life cycle states, on page 2-13. If cell state cannot be determined, a note indicates the primary (or secondary) cell is lost. • Smart cell's general current life cycle state: <ul style="list-style-type: none"> – green (normal state): ASSIGNED, CLOSED, FREE – yellow (maintenance state): DISCOVERY, COMPLETE_PROCESSING, BACKING_UP, SYNC_WAIT, RESET, RESTORE – red (failure state): DEAD, SUSPENDED

Table 2-97: View Cell Space view features (continued)

Feature	Description
Unaffiliated Smart Cells	Smart cells not currently affiliated with any domain (not belonging to a smart cell group). These are reserve cells you can use when needed. Cell descriptions are the same as those in domain lists. Unaffiliated cells are in the FREE or RESET life cycle state.

Related Views

- The Smart Cell Groups for Domain view provides much of the smart cell information in the View Cell Space view. See [Displaying the Smart Cell Groups for Domain view, on page 2-23](#).

Table 2-98: Links to View Cell Space view

Origin	Link
left menu	View Cell Space

Table 2-99: Links from View Cell Space view

Destination	Link
Agent view, on page 2-118	<ul style="list-style-type: none"> • host name • Back to Agent View
MBean view, on page 2-117	Back to MBean View

Displaying hosts

In the View Cell Space view, under SMTP Portals, HTTP Portals, MetaServer, or TSC-NAT, click a name. The Agent view appears.

Displaying host names of smart cells in domain-affiliated smart cell groups

1. In the View Cell Space view, find smart cell's domain.

2. Find smart cell's smart cell group identification number. Host names of smart cells in the smart cell group appear beneath the smart cell group identification number.

Displaying domain-affiliated smart cells

1. In the View Cell Space view, find smart cell's domain.
2. Find smart cell's smart cell group identification number.
3. Click smart cell's name. The Agent view appears.

Displaying unaffiliated smart cells

Unaffiliated smart cells are “free” and contain no data.

To display unaffiliated smart cells, scroll to the bottom of the View Cell Space view.

To display the Agent view:

1. Scroll to the bottom of the View Cell Space view.
2. Find smart cell's smart cell group identification number.
3. Click smart cell's name.

Determining if smart cells are primary or secondary cells

1. In the View Cell Space view, find smart cell's domain.
2. Find smart cell's smart cell group identification number. Primary and secondary cells are designated by the first letter in the smart cell group identification number:
 - P (primary)
 - S (secondary)

Determining if smart cells are used for replication

1. In the View Cell Space view, find smart cell's domain.

2. Find smart cell's smart cell group identification number. Replicas are designated by the first letter in the smart cell group identification number:
 - R1 (primary replica)
 - R2 (secondary replica)

Restoring data on failed smart cells

To restore data on a failed smart cell, you must have at least one free smart cell. If only one smart cell in a group failed, clone a smart cell instead (see [Smartcell Cloning view, on page 2-36](#)).

To restore a smart cell, the following must occur:

- Its domain has `DataBackupEnabled=true` set in the `Domain.jcml` configuration file.
- Its group was assigned in this system at one time.
- It is marked as missing in the `ViewCellState` table *or* no record exists in the `ViewCellState` table.

Note: Rebuilding the index on the smart cell takes a significant amount of time depending on the amount of data being restored.

If both smart cells in a group failed, perform the following:

1. In the View Cell Space view, scroll to the Unaffiliated SmartCells area, and verify that at least one free smart cell exists.
2. Locate the primary controller:
 - a. Under MetaServer, click the link to the primary or main controller (metaserver). The Agent view appears.
 - b. From the MBean list, click ProvisionerMBean. The MBean view appears.
 - c. Verify the ProvisionerMasterBackupStatus attribute is set to Master Provisioner. If it is set to Backup Provisioner, return to the View Cell Space view, click the link to the other metaserver, and repeat the previous steps.

4. Determine which smart cells failed and can be restored:
 - a. In the MBean view for the primary controller, click the button next to `ListBrokenGroups`. Groups that failed and have not been recovered are listed.
 - b. Copy GroupIDs and Roles of broken groups.
 - c. Click Back to MBean view.
4. Restore the smart cell:
 - a. Under the `RestoreSmartCellUsingGroupIDAndRole` attribute, enter the group ID in the first field and the role in the second field.
 - b. Click Invoke.
 - c. If the restore is successful, a confirmation message appears. Note the restore target information.
 - d. If an error occurs, verify that the group ID and role are correct. If the information is correct, verify that the smart cell needs restoring and there is a free smart cell.
5. Verify that the restore process is running correctly or has completed:
 - a. In the View Cell Space view, locate the restored smart cell listed in the confirmation message.
 - b. If the smart cell assigned is not in the restore state, the restore process completed and no further action is required. Otherwise, click the link to the smart cell in the restore state.
 - c. From the MBean list, click `BackupSystemMBean`. The MBean view appears.
 - d. Verify that the `RunningState` attribute is 3 and the `FailureReason` attribute is No Failure. This indicates the restore process is occurring normally.

If the `RunningState` attribute is 5, the restore process failed. Check the `FailureReason` attribute for the cause.

MBean view

This view shows operations (methods) and attributes exposed by a particular managed object (MBean or JBoss component) for remote management purposes.

Note: *Do not modify* settings in this view. For monitoring purposes, you normally do *not* need to use this view. It is intended only for installers and advanced system administrators.

You can view the life cycle state change history for an individual smart cell in the MBean view for the SmartCellStateControllerMBean of the smart cell.

In the View Cell Space view, go to the smart cell's Agent view, and go to the MBean view for the SmartCellStateControllerMBean.

Related Views

- [Displaying all services running on specific hosts, on page 2-51](#)

Table 2-100: Links **to** MBean view

Origin	Link
Agent view, on page 2-118	any listed object

Table 2-101: Links **from** MBean view

Destination	Link
Agent view, on page 2-118	Back to Agent View
Array view (you normally do <i>not</i> need to use this view)	various

Agent view

This view shows managed objects (MBeans or JBoss components) currently running on a particular host machine.

Note: *Do not modify* settings in this view. For monitoring purposes, you normally do *not* need to use this view. It is intended only for installers and advanced system administrators.

Noteworthy MBeans include:

- For smart cells
 - ArchiveServiceMBean (document archiving)
 - Indexer (document indexing)
 - SmartCellStateControllerMBean
- For SMTP services
 - SMTPService

Related Views

- [Displaying all services running on specific hosts, on page 2-51](#)

Table 2-102: Links to Agent view

Origin	Link
Displaying all services running on specific hosts, on page 2-51	<ul style="list-style-type: none"> • Back to Agent View • host name
MBean view, on page 2-117	Back to Agent View

Table 2-103: Links from Agent view

Destination	Link
MBean view, on page 2-117	any listed object
Agent Administration view (you normally do <i>not</i> need to use this view)	Admin (button)

Warnings folder

All Warnings view

This view displays a program stack trace for each exception occurring on each host in a given host group.

Note: For monitoring purposes, you normally do *not* need to use this view. It is intended only for troubleshooting and configuration by installers and advanced system administrators.

Table 2-104: Links to All Warnings views

Origin	Link
left navigation menu	All Warnings
left navigation menu	HTTP Warnings
left navigation menu	Smtplib Warnings
left navigation menu	Metaserver Warnings
left navigation menu	Smartcell Warnings
left navigation menu	Labfirewall Warnings

Table 2-105: Links from All Warnings view

Destination	Link
System Status view, on page 2-20	Return to Summary

Additional views

Hostgroup Information view

This view provides information about service monitoring performance for a given host group. Except for the addition of access to Hostgroup Commands, this view provides the same information as the Nagios Stats view, filtered for a single host group.

Table 2-106: Hostgroup Information view features

Feature	Description
Time Frame/ Checks Completed	Number and percentage of PCC services checked in indicated time frames (since PCC startup or in the last 1, 5, 15, or 60 minutes).
Check Metric/Min/Max/Average <ul style="list-style-type: none">• Execution Time• Latency	Minimum, maximum, and average times: <ul style="list-style-type: none">• it took to check service• between time service check was scheduled and time it was executed PCC <i>does not use</i> % State Change.
Hostgroup Commands	Links to commands that perform actions on this host group. See Hostgroup Commands section, on page 2-123 for more information. <i>Note:</i> Commands that disable (notifications, status checks, and so on) override commands that enable. For example, suppose you disable service checks for a particular host group using the Hostgroup Information view (command Disable checks of all services in this hostgroup), but enable checks for all services using the Nagios Info view (command Start executing service checks). Services for the host group are <i>not</i> checked because disabling overrides enabling.

The Passive Service Checks charts are *not used*; all PCC service checks are active.

Related Views

- See [Nagios Info view, on page 2-68](#), for information about global commands affecting all host groups.
- The Nagios Stats view presents the same monitoring performance information, but for all host groups; and it does not have Hostgroup Commands. See [Scheduling Queue view, on page 2-73](#).
- [Tactical Monitoring view, on page 2-50](#), also provides limited information about monitoring performance.

Table 2-107: Links to Hostgroup Information view

Origin	Link
Status Summary view, on page 2-17	host group abbreviation, in parentheses, such as (sc).
Service Overview view, on page 2-58	host group abbreviation, in parentheses, such as (sc).
Status Grid view, on page 2-141	host group abbreviation, in parentheses, such as (sc).

Table 2-108: Links from Hostgroup Information view

Destination	Link
Service Detail view, on page 2-53 , for host group	View Status Detail For This Hostgroup
Service Overview view, on page 2-58 , for host group	View Service Overview For This Hostgroup
Status Grid view, on page 2-141 , for host group	View Status Grid For This Hostgroup
Availability view, on page 2-85 , for host group	View Availability For This Hostgroup
External Command Interface view, on page 2-143	specific Hostgroup Commands

Hostgroup Commands section

To execute a command:

1. Click on any link listed in Table 2-109. The External Command Interface view for that command appears. See [External Command Interface view, on page 2-143](#), for more information.
2. Specify appropriate information. See command descriptions in Table 2-109 for more information.
3. Click Commit to save changes, or click Reset to clear input fields.

Table 2-109: Hostgroup Commands section, Hostgroup Information view

Command link	Description
Schedule downtime for all hosts in a specific hostgroup	<p>Schedules downtime for all hosts in a particular hostgroup. During scheduled downtimes, Nagios does not send notifications about hosts. When scheduled downtimes expire, Nagios sends notifications for hosts as normal. Scheduled downtimes are preserved across program shutdowns and restarts.</p> <p>The following fields are required:</p> <ul style="list-style-type: none">• Hostgroup Name• Author (Your Name)• Comment• Start Time (mm/dd/yyyy hh:mm:ss)• End Time (mm/dd/yyyy hh:mm:ss) <p>If you select the Fixed check box, downtime is in effect between specified start and end times. If you do not select the Fixed check box, Nagios treats this as “flexible” downtime. Flexible downtime starts when a host goes down or becomes unreachable (sometime between specified start and end times) and lasts for specified duration. Duration fields do not apply to fixed downtime.</p>

Table 2-109: Hostgroup Commands section, Hostgroup Information view

Command link	Description
Schedule downtime for all services in a specific hostgroup	<p>Schedules downtime for all services in a particular hostgroup. During scheduled downtimes, Nagios does not send notifications about services. When scheduled downtimes expire, Nagios sends notifications for services as normal. Scheduled downtimes are preserved across program shutdowns and restarts.</p> <p>Scheduling downtime for services does not automatically schedule downtime for the hosts those services are associated with.</p> <p>The following fields are required:</p> <ul style="list-style-type: none"> • Hostgroup Name • Author (Your Name) • Comment • Start Time (mm/dd/yyyy hh:mm:ss) • End Time (mm/dd/yyyy hh:mm:ss) <p>If you select the Fixed check box, downtime is in effect between specified start and end times. If you do not select the Fixed check box, Nagios treats this as “flexible” downtime. Flexible downtime starts when a service enters a non-OK state (sometime between specified start and end times) and lasts as long as specified duration. Duration fields do not apply to fixed downtime.</p> <p>To schedule the same downtime for all hosts in this host group, select the Schedule Downtime for Hosts Too check box.</p>
Enable notifications for all hosts in a specific hostgroup	<p>Enables notifications for all hosts in specified hostgroup. Notifications are only sent for host state types defined in your host definitions.</p> <p>Enter information in the Hostgroup Name field.</p>
Disable notifications for all hosts in a specific hostgroup	<p>Prevents notifications from being sent for all hosts in specified hostgroup. You must re-enable notifications for all hosts in this hostgroup before alerts are sent again.</p> <p>Enter information in the Hostgroup Name field.</p>

Table 2-109: Hostgroup Commands section, Hostgroup Information view

Command link	Description
Enable notifications for all services in a specific hostgroup	<p>Enables notifications for all services in specified hostgroup. Notifications are only sent for service state types defined in your service definitions.</p> <p>Enter information in the Hostgroup Name field.</p> <p>To enable notifications for all hosts in this hostgroup, select the Enable for Hosts Too check box.</p>
Disable notifications for all services in a specific hostgroup	<p>Prevents notifications from being sent for all services in specified hostgroup. You must re-enable notifications for all services in this hostgroup before any alerts are sent again.</p> <p>Enter information in the Hostgroup Name field.</p> <p>To disable notifications for all hosts in this hostgroup, select the Disable for Hosts Too check box.</p>
Enable checks of all services in a specific hostgroup	<p>Enables all service checks in specified hostgroup.</p> <p>Enter information in the Hostgroup Name field.</p> <p>To enable checks of all hosts in this hostgroup, select the Enable for Hosts Too check box.</p>
Disable checks of all services in a specific hostgroup	<p>Disables all service checks in specified hostgroup. When a service is disabled, Nagios does not monitor the service or send notifications for the service. To have Nagios check services again, you must re-enable services.</p> <p>Disabling service checks may not prevent notifications from being sent about the host those services are associated with.</p> <p>Enter information in the Hostgroup Name field.</p> <p>To disable checks of all hosts in this hostgroup, select the Disable for Hosts Too check box.</p>

Host Information view

This view provides status information for a given host.

Table 2-110: Host Information view features


Feature	Description
heading	Full and abbreviated names of host, and host IP address. For example: <ul style="list-style-type: none"> SmartCellMachines:sc-s1-172-1.mycorp.com: Full host name sc-s1-172-1: Abbreviated host name 10.0.172.1: IP address SmartCellMachines:1: First host in host group SmartCellMachines
Host State Statistics	Amount and percentage of time this host has had each host status value, and total time. See Host and service status values, on page 2-14 .
Host Commands	Links to commands that perform actions on host. See Host Commands section, on page 2-128 , for more information. <i>Note:</i> Commands that disable (notifications, status checks, and so on) override commands that enable. For example, suppose you disable checks for all services on a particular host using the Host Information view (command Disable checks of all services on this host), but enable checks for all services on all hosts using the Nagios Info view (command Start executing service checks). Services for the particular host are <i>not</i> checked because disabling overrides enabling.
Host Comments	Comments for host. Comments are notes to yourself or other system administrators. The following information is shown for each comment: <ul style="list-style-type: none"> Entry Time: Time comment was added. Author: Who entered comment. Comment: Comment text. Comment ID: Unique sequential identifier, incremented whenever a comment is added. Persistent: Yes. PCC comments are always persistent. Actions: Click the wastebasket icon () to delete comment.

Table 2-110: Host Information view features (continued)

Feature	Description
Host State Information	<p>Host status information:</p> <ul style="list-style-type: none"> • Host Status, Status Information, Last Status Check: Current status value, with additional status information and time of last status check. • Host Checks Enabled?: If host is checked for status. Change this value with the associated host command (see Host Commands section, on page 2-128). • Last State Change, Current State Duration: Time of latest status value change, and how long host has had current status value. • Last Host Notification, Current Notification Number: Time and number of latest notification from host. • Host Notifications Enabled?: If notifications are currently enabled for host. Change this value with the associated host command (see Host Commands section, on page 2-128). This is overridden by the global Enable/Disable Notifications command. See Nagios Info view, on page 2-68. • In Scheduled Downtime?: If current time is scheduled downtime for host. • Last Update: Time host was last checked.

Related Views

- See [Nagios Info view, on page 2-68](#), for information about global commands affecting *all* hosts
- [Comments view, on page 2-63](#)

Table 2-111: Links to Host Information view


Origin	Link
Service Detail view, on page 2-53	specific host name
Service Problems view, on page 2-61	specific host name
Host Detail view, on page 2-56	specific host name
Service Overview view, on page 2-58	Actions icon View Extended Information For This Host ()
Scheduling Queue view, on page 2-73	specific host name

Table 2-111: Links to Host Information view (continued)

Origin	Link
Alerts Summary view, on page 2-100	specific host name
Notifications view, on page 2-89	specific host name
Status Grid view, on page 2-141	specific host name
Service Information view, on page 2-133	View Information For This Host

Table 2-112: Links from Host Information view

Destination	Link
Service Detail view, on page 2-53, for host	View Status Detail For This Host
Alerts History view, on page 2-97, for host	View Alert History For This Host
Alerts folder, on page 2-94, for host, for last 24 hours	View Trends For This Host
Creating availability reports, on page 2-88, for host	View Alert Histogram For This Host
Availability view, on page 2-85, for host	View Availability Report For This Host
Notifications view, on page 2-89, for host	View Notifications For This Host
External Command Interface view, on page 2-143	command (Host Commands)

Host Commands section

To execute a command:

1. Click on any link listed in Table 2-113. The External Command Interface view for that command appears. See [External Command Interface view, on page 2-143](#), for more information.
2. Specify appropriate information. See command descriptions in Table 2-113 for more information.
3. Click Commit to save changes, or click Reset to clear input fields.

Table 2-113: Host Commands section, Host Information view

Command Link	Description
Disable checks of a specific host	<p>Temporarily prevents Nagios from checking a particular host's status. If Nagios must check host's status, it assumes the host is in the same state it was in before checks were disabled.</p> <p>Enter information in the Host Name field.</p>
Acknowledge a specific host problem	<p><i>Note:</i> This option appears only if the host status is not OK.</p> <p>Acknowledges host problems. Future notifications about problems are temporarily disabled until host changes state (for example, recovers). Contacts for host receive an acknowledgement notification, so they are aware someone is working on the problem. A comment is also added to host. Enter your name and a brief description of your actions in the comment field.</p> <p>The following fields are required:</p> <ul style="list-style-type: none"> • Host Name • Author (Your Name) • Comment <p>To send acknowledgement notifications to appropriate contacts, select the Send Notification check box.</p> <p>To retain comments between Nagios restarts, select the Persistent check box.</p>
Disable notifications for a specific host	<p>Prevents notifications from being sent for specified host. You must re-enable notifications for host before alerts are sent again. This command <i>does not</i> disable notifications for services associated with host.</p> <p>Enter information in the Host Name field.</p>

Table 2-113: Host Commands section, Host Information view (continued)


Command Link	Description
Schedule downtime for a specific host	<p>Schedules downtime for a particular host. During specified downtimes, Nagios does not send notifications about host. When scheduled downtimes expire, Nagios sends notifications for host as normal. Scheduled downtimes are preserved across program shutdowns and restarts. The following fields are required:</p> <ul style="list-style-type: none"> • Host Name • Author (Your Name) • Comment • Start Time (mm/dd/yyyy hh:mm:ss) • End Time (mm/dd/yyyy hh:mm:ss) <p>If you select the Fixed check box, downtime is in effect between specified start and end times. If you do not select the Fixed check box, Nagios treats this as “flexible” downtime. Flexible downtime starts when host goes down or becomes unreachable (sometime between specified start and end times) and lasts for specified duration. Duration fields do not apply for fixed downtime.</p>
Disable notifications for all services on a specific host	<p>Prevents notifications from being sent for all services on specified host. You must re-enable notifications for all services associated with host before alerts are sent again. This <i>does not</i> prevent notifications from being sent about host, unless you check the Disable for host too check box. Enter information in the Host Name field.</p>
Enable notifications for all services on a specific host	<p>Enables notifications for all services on specified host. Notifications are only sent for service state types defined in your service definition. This <i>does not</i> enable notifications for host, unless you check the Enable for host too check box. Enter information in the Host Name field.</p>

Table 2-113: Host Commands section, Host Information view (continued)


Command Link	Description
Schedule an immediate check of all services on a specific host	<p>Schedules immediate check of all services on specified host. Checks are <i>scheduled</i> immediately, not necessary executed immediately. If Nagios falls behind in its scheduling queue, it checks services queued prior to these services.</p> <p>If you select the Force check box, Nagios forces a check of all services on host regardless of when scheduled checks occur and whether or not checks are enabled for those services.</p> <p>Enter information in the Host Name field.</p>
Disable checks of all services on a specific host	<p>Disables all service checks associated with specified host. When a service is disabled, Nagios does not monitor the service and stops sending notifications for specified service. To have Nagios check service again, you must re-enable service.</p> <p>Disabling service checks may not prevent notifications from being sent about host those services are associated with. This <i>does not</i> disable checks of host, unless you check the Disable for host too check box.</p> <p>Enter information in the Host Name field.</p>
Enable checks of all services on a specific host	<p>Enables all service checks associated with specified host. This <i>does not</i> enable checks of host, unless you check the Enable for host too check box.</p> <p>Enter information in the Host Name field.</p>
Disable event handler for a specific host	<p>Temporarily prevents Nagios from running the host event handler for specific host.</p> <p>Enter information in the Host Name field.</p>
Disable flap detection for a specific host	<p>Disables flap detection for specific host.</p> <p>Enter information in the Host Name field.</p>

Adding comments for specific hosts

If you work with other administrators, you might find it useful to share information about a host that has problems. If you do not check the **Persistent** check box, comments are automatically deleted the next time Nagios is restarted.

1. In the Host Comments section, click the Add new comment link (). The External Command Interface appears.
2. In the Command Options section, enter the following information:
 - Host Name
 - Author (Your Name)
 - Comment
3. To retain comment between Nagios restarts, click to select the Persistent check box.
4. Click Commit to save changes, or click Reset to clear input fields.

Deleting all comments for specific hosts

1. In the Host Comments section, click the Delete all comments link (). The External Command Interface appears.
2. In the Command Options section, enter information in the Host Name field.
3. To retain comments between Nagios restarts, click to select the Persistent check box.
4. Click Commit to save changes, or click Reset to clear input fields.

Service Information view

This view provides status information for a given service.

Table 2-114: Service Information view features


Feature	Description
heading	Name of service. Full and abbreviated names of host and host IP address. See Host Information view, on page 2-126 .
Service State Statistics	Amount and percentage of time service has had each service status value, and total time. See Host and service status values, on page 2-14 .
Service Commands	<p>Links to commands that perform actions on service. See Service Commands section, on page 2-135, for more information.</p> <p><i>Note:</i> Commands that disable (notifications, status checks, and so on) override commands that enable. For example, suppose you disable checks for a particular service, such as PING, using the Service Information view (command Disable checks of this service), but enable checks for all services using the Nagios Info view (command Start executing service checks). The particular service (PING) is <i>not</i> checked, because disabling overrides enabling.</p>
Service Comments	<p>All comments for service. Comments are notes you make to yourself or other system administrators. The following information is shown for each comment:</p> <ul style="list-style-type: none"> • Entry Time: Time comment was added. • Author: Who entered comment. • Comment: Comment text. • Comment ID: Unique sequential identifier, incremented whenever a comment is added. • Persistent: Yes. PCC comments are always persistent. • Actions: Click the wastebasket icon () to delete comment.

Table 2-114: Service Information view features (continued)

Feature	Description
Service State Information	<p>Status information for service:</p> <ul style="list-style-type: none"> • Current Status, Status Information: Current service status value, and additional status information. • Last Check Time, Next Scheduled Active Check: Times of latest and next scheduled status checks. • Current Attempt: Number of successful attempts and total number of attempts to check service. • Latency: Time elapsed from when latest service check was scheduled to when it was executed. • Check Duration: Duration of latest status check. • Service Checks Enabled?: If service is checked for status. You can change this value with the associated service command (see Service Commands section, on page 2-135). • Last State Change, Current State Duration: Time service last changed status value, and how long it has had current status value. • Last Host Notification, Current Notification Number: Time and number of latest notification from service. • Service Notifications Enabled?: If notifications are currently enabled for service. You can change this value with the associated service command (see Service Commands section, on page 2-135). This is overridden by the global Enable/Disable Notifications command. See Nagios Info view, on page 2-68. • In Scheduled Downtime?: If current time is scheduled downtime for host of this service. • Last Update: Time service was last checked. <p>Last Check Type and State Type are <i>not used</i> by the PCC.</p>

Related Views

- See [Nagios Info view, on page 2-68](#), for information about global commands affecting *all* services.
- [Comments view, on page 2-63](#).

Table 2-115: Links to Service Information view

Origin	Link
Service Detail view, on page 2-53	service name

Table 2-115: Links to Service Information view (continued)

Origin	Link
Service Problems view, on page 2-61	service name
Scheduling Queue view, on page 2-73	service name
Alerts Summary view, on page 2-100	service name
Notifications view, on page 2-89	service name
Status Grid view, on page 2-141	service name

Table 2-116: Links from Service Information view

Destination	Link
Host Information view, on page 2-126	View Information For This Host
Service Detail view, on page 2-53, for host	View Status Detail For This Host
Alerts History view, on page 2-97, for service	View Alert History For This Service
Alerts folder, on page 2-94, for service, for last 24 hours	View Trends For This Service
Creating availability reports, on page 2-88, for service	View Alert Histogram For This Service
Availability view, on page 2-85, for service	View Availability Report For This Service
Notifications view, on page 2-89, for service	View Notifications For This Service
External Command Interface view, on page 2-143	command (Service Commands)

Service Commands section

To execute a command:

1. Click on any link listed in Table 2-117. The External Command Interface view for that command appears. See [External Command Interface view, on page 2-143](#), for more information.

2. Specify appropriate information. See command descriptions in Table 2-117 for more information.
3. Click Commit to save changes, or click Reset to clear input fields.

Table 2-117: Service Commands section, Service Information view

Command link	Description
Acknowledge a specific service problem	<p><i>Note:</i> This option appears only if service status is not OK.</p> <p>Acknowledges service problem. When service problem is acknowledged, future notifications about problems are temporarily disabled until service changes state (for example, recovers). Contacts for service receive acknowledgement notifications, so they are aware someone is working on the problem.</p> <p>A comment is also added to service. Enter your name and brief description of your actions to the comment field.</p> <p>The following fields are required:</p> <ul style="list-style-type: none">• Host Name• Service• Author (Your Name)• Comment <p>To retain service comment between restarts of Nagios, select the Persistent check box.</p> <p>To send acknowledgement notifications to appropriate contacts, select the Send Notification check box.</p>
Disable notifications for a specific service	<p>Prevents notifications from being sent for specified service. You must re-enable notifications for service before alerts are sent again.</p> <p>Enter information in the Host Name field.</p>

Table 2-117: Service Commands section, Service Information view (continued)

Command link	Description
Delay next service notification	<p>Delays next problem notification sent for specified service. Notification delay is disregarded if service changes state before next notification is scheduled to be sent. This command has no effect if service is currently in an OK state.</p> <p>The following fields are required:</p> <ul style="list-style-type: none"> • Host Name • Service • Notification Delay (minutes from now)
Schedule downtime for a specific service	<p>Schedules downtime for a particular service. During specified downtimes, Nagios does not send notifications about service. When scheduled downtimes expire, Nagios sends notifications for service as normal. Scheduled downtimes are preserved across program shutdowns and restarts.</p> <p>The following fields are required:</p> <ul style="list-style-type: none"> • Host Name • Service • Author (Your Name) • Comment • Start Time (mm/dd/yyyy hh:mm:ss) • End Time (mm/dd/yyyy hh:mm:ss) <p>If you select the Fixed check box, downtime is in effect between specified start and end times. If you do not select the Fixed check box, Nagios treats this as “flexible” downtime. Flexible downtime starts when service enters a non-OK state (sometime between specified start and end times) and lasts as long as specified duration. Duration fields do not apply to fixed downtime.</p>

Table 2-117: Service Commands section, Service Information view (continued)


Command link	Description
Disable checks of a specific service	<p>Disables service checks. When service is disabled, Nagios does not monitor service and stops sending notifications for specified service while it is disabled. To have Nagios check service again, you must re-enable service.</p> <p>Disabling service checks may not prevent notifications from being sent about host those services are associated with.</p> <p>The following fields are required:</p> <ul style="list-style-type: none"> • Host Name • Service
Re-schedule the next check of a specific service	<p>Reschedules next check of service. Nagios requeues service to be checked at specified time.</p> <p>If you select the Force check box, Nagios forces a service check regardless of what time scheduled check occurs and whether or not checks are enabled for service.</p> <p>The following fields are required:</p> <ul style="list-style-type: none"> • Host Name • Service • Check Time
Submit passive check result for this service	<p>Submits a passive check result for service. This command is particularly useful for resetting security-related services to OK states after they have been handled.</p> <p>The following fields are required:</p> <ul style="list-style-type: none"> • Host Name • Service • Check Result (drop-down menu) • Check Output
Stop accepting passive checks for this service	<p>Stops Nagios from accepting passive service check results found in the external command file for service. All passive check results found for service are ignored.</p> <p>The following fields are required:</p> <ul style="list-style-type: none"> • Host Name • Service

Table 2-117: Service Commands section, Service Information view (continued)


Command link	Description
Disable event handler for a specific service	Temporarily prevents Nagios from running the service event handler for service. The following fields are required: <ul style="list-style-type: none">• Host Name• Service
Disable flap detection for a specific service	Disables flap detection for service. The following fields are required: <ul style="list-style-type: none">• Host Name• Service

Adding comments for specific services

If you work with other administrators, you might find it useful to share information about a host or service that is having problems.

1. In the Service Comments section, click the Add new comment link (). The External Command Interface appears.
2. In the Command Options section, enter the following information:
 - Host Name
 - Service
 - Author (Your Name)
 - Comment
3. To retain comments between Nagios restarts, click to select the Persistent check box.
4. Click Commit to save changes, or click Reset to clear input fields.

Deleting all comments for specific services

1. In the Service Comments section, click the Delete all comments link ().
The External Command Interface appears.
2. In the Command Options section, enter the following information:
 - Host Name
 - Service
3. Click Commit to save changes, or click Reset to clear input fields.

Status Grid view

This view provides a high-level summary of hosts and services, organized by host group. Each host and service is listed, and its status value is shown by color coding (see [Host and service status values, on page 2-14](#)). To see details, click host or service entry.

The charts Host Status Totals and Service Status Totals of the Status Grid view are the same as those of the Status Summary view. See [Status Summary view, on page 2-17](#).

Table 2-118: Status Grid view, Hostgroup features

Feature	Description
host group	Host group name and abbreviation.
Host	Hosts in host group.
Services	Names of services running on each host in host group.

Table 2-119: Links to Status Grid view

Origin	Link
Status Summary view, on page 2-17	View Status Grid For All Host Groups
Host Detail view, on page 2-56	View Status Grid For All Host Groups
Host Problems view, on page 2-62	View Status Grid For All Host Groups
Service Overview view, on page 2-58	View Status Grid For All Host Groups
Service Detail view, on page 2-53 , when main heading is Service Status Details For All Host Groups	View Status Grid For All Host Groups
Service Detail view, on page 2-53 , for single host group	View Status Grid For This Host Group
Hostgroup Information view, on page 2-121 , for single host group	View Status Grid For This Hostgroup
Status Grid view, for single host group	View Status Grid For All Host Groups

Table 2-120: Links from Status Grid view

Destination	Link
Host Detail view, on page 2-56	View Host Status Detail . . .
Service Detail view, on page 2-53	View Service Status Detail . . .
Service Overview view, on page 2-58	View Service Overview . . .
Status Summary view, on page 2-17	View Status Summary . . .
Status Grid view, for all host groups	View Status Grid For All Host Groups, when viewing Status Grid for single host group

Displaying specific hostgroups


Click host group name, such as Smart Cells. The Service Detail view appears. See [Service Detail view, on page 2-53](#).

Click host group's parenthetical abbreviation, such as (sc). The Hostgroup Information view appears. See [Hostgroup Information view, on page 2-121](#).

Displaying specific hosts

In the Host column, click host group name, such as SmartCells. The Host Information view appears. See [Host Information view, on page 2-126](#).

Displaying all services running on specific hosts

In the Host column, click host status-signal icon (). The Service Detail view appears. See [Service Detail view, on page 2-53](#).

Displaying specific services

In the Service column, click service name. The Service Information view appears. See [Service Information view, on page 2-133](#).

External Command Interface view

Use this view to run commands that perform actions. Some commands allow or require additional command information. Fields labeled in red are required input. To run a command, enter command information, and click Commit. Reset clears all input fields.

Some commands are applicable to individual hosts or services, all hosts of a host group, or all services running on a host.

Table 2-121: External commands

Shut down (stop) Nagios process (PCC monitoring), so RISS is no longer monitored.

Restart Nagios process (PCC monitoring).

Enable or disable sending notifications for hosts or services. See [Example: Enabling or disabling notifications, on page 2-144](#).

Enable or disable host or service checks (monitoring).

Add host or service comments. See [Example: Adding comments, on page 2-144](#).

Schedule host or service downtimes.

Schedule immediate check of all services on host.

Reschedule next check of service.

Note: Commands that disable (notifications, status checks, and so on) override commands that enable. For example, suppose you disable checks for a particular service, such as PING, using the Service Information view (command Disable checks of this service), but enable checks for all services using the Nagios Info view (command Start executing service checks). That particular service (PING) is *not* checked because disabling overrides enabling.

Example: Enabling or disabling notifications

If you click Disabled next to Notifications in the Tactical Overview view (see [Tactical Monitoring view, on page 2-50](#)), which indicates notifications are currently disabled, the External Command Interface view appears with the message You are requesting to enable notifications. No additional command information is required; just click Commit.

Example: Adding comments

If you click Add a new host (service) comment in the Comments view (see [Comments view, on page 2-63](#)), the External Command Interface view appears with the message You are requesting to add a host (service) comment. Enter a host and service name, your name, and your comment. The Persistent check box is *not used*. (PCC comments are always persistent: they are not deleted when the Control Center shuts down.) Click Commit to execute the command.

Example: Acknowledging problems

Use the Acknowledge this host/service problem command to notify others you are working on a problem. This command is available in the Host/Service Commands box of the Host/Service Information view whenever a host or service has a problem (see [Host Information view, on page 2-126](#), and [Service Information view, on page 2-133](#)). Use the command Remove problem acknowledgement to remove problem acknowledgements.

After acknowledging a problem, problem notifications for that host or service is disabled until it recovers. Contacts for the host or service receive notification of your acknowledgement (unless you clear the Send Notification check box in the External Command Interface view when acknowledging).

Related Views

- [Replication view, on page 2-39](#)
- [Tactical Monitoring view, on page 2-50](#)
- [Comments view, on page 2-63](#)
- [Nagios Info view, on page 2-68](#)
- [Hostgroup Information view, on page 2-121](#)
- [Host Information view, on page 2-126](#)

- [Service Information view, on page 2-133](#)

Table 2-122: Links to External Command Interface view

Origin	Link
Tactical Monitoring view, on page 2-50	Enabled/Disabled
Comments view, on page 2-63	Add a new host/service comment
Host Downtime view, on page 2-65	Schedule host/service downtime
Nagios Info view, on page 2-68	commands (Process Commands)
Scheduling Queue view, on page 2-73	Actions for specific service
Hostgroup Information view, on page 2-121	commands (Hostgroup Commands)
Host Information view, on page 2-126	commands (Host Commands)
Service Information view, on page 2-133	commands (Service Commands)

Links **from** External Command Interface view: none

CHAPTER 3

Platform Account Manager

This chapter explains how to use the Platform Account Manager (PAM) to provision and update user accounts.

This chapter contains these topics:

- [PAM overview, on page 3-2](#)
- [Performing basic PAM tasks, on page 3-8](#)
- [Managing user accounts, on page 3-14](#)
- [Managing repositories, on page 3-19](#)
- [Managing access control lists \(ACLs\), on page 3-23](#)
- [Managing routing rules, on page 3-27](#)
- [Managing simple routing rules, on page 3-31](#)
- [Managing routing filters, on page 3-34](#)
- [Example: Integrating new department, on page 3-39](#)

PAM overview

Use the **Platform Account Manager (PAM)** to view and update individual user accounts for unusual circumstances on the HP StorageWorks Reference Information Storage System (RISS). Initial setup and routine addition and deletion of user accounts occurs automatically through synchronization with Windows Active Directory.

RISS archives emails and other documents in one or more repositories. A **repository** is a virtual collection of documents associated with a given user by **routing rules** (storing) and **access control lists** (retrieving). Users can find and retrieve archived documents they can access.

User accounts

Use PAM to update user accounts as follows:

- add users not imported through dynamic account synchronization (DAS)
- add special-purpose repositories
- add or modify routing rules
- add users to new and existing access control lists

Note: You can view user accounts on replica domains, but you cannot use PAM to add or edit them. Fields cannot be edited and action buttons are unavailable when you select a domain that is a replica of another domain.

Installing PAM

PAM runs on Microsoft Windows platforms. To install PAM, copy the `pam` directory from the Utilities CD to a Windows drive.

Logging in to PAM

1. Navigate to the `pam/bin` directory on your Windows machine.
2. Double-click `pam.bat`. The Login dialog box appears.
3. Enter the following:
 - User Name: Your user name. (You must be a user with administrative privileges to use PAM.)
 - User Password: Your password. To change your password, use the RISS Web Interface (choose Preferences).
 - PCC NAT Host: Name or IP address of the PCC NAT host.
 - PCC Admin Name: `admin`
 - PCC Admin Password: Password for accessing the Platform Control Center (PCC).
4. Click OK. The Platform Account Manager window appears (see [PAM window, on page 3-4](#)).

PAM window

After logging in to PAM (see [Logging in to PAM, on page 3-3](#)), the Platform Account Manager window appears.

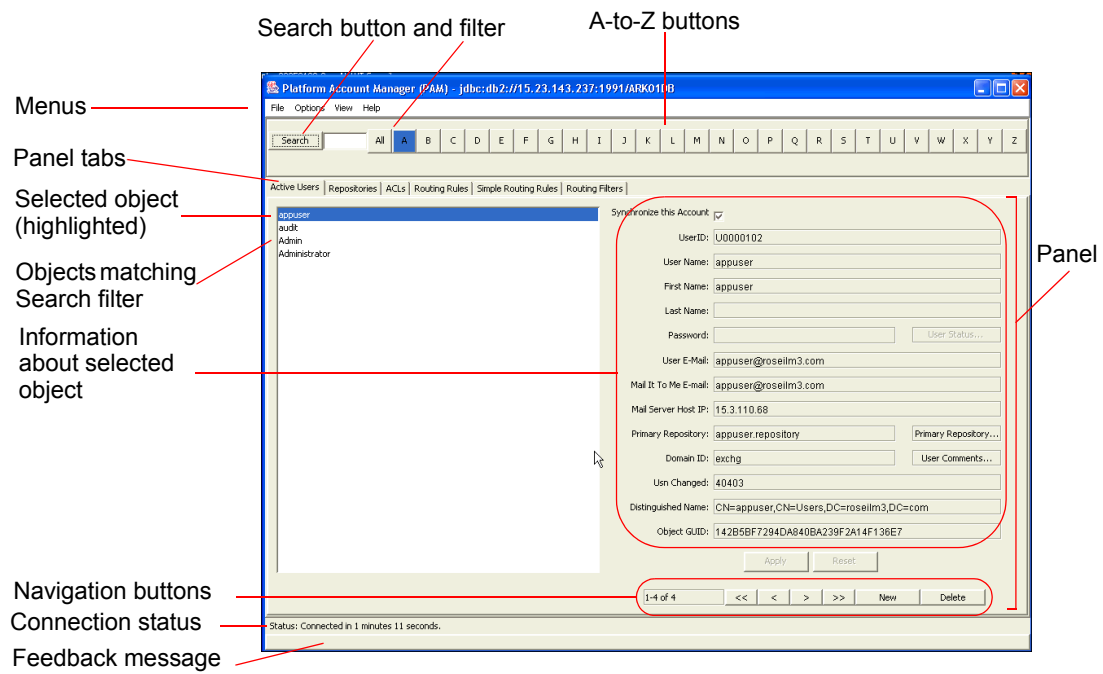


Figure 3-1: Platform Account Manager window

Table 3-1: Platform Account Manager window features

Feature	Description
File menu	• Exit – Exits PAM.

Table 3-1: Platform Account Manager window features (continued)

Feature	Description
Options menu	<ul style="list-style-type: none"> • Show Users – Determines registered users displayed in the Users panel. Options are: <ul style="list-style-type: none"> – All Users – Shows all users of the system. – Active Users – Shows only users who are allowed to log in (active Outlook Integration Users and active Non-Outlook Integration Users). – Inactive Users – Shows only users who are not allowed to log in. – Outlook Integration Users – Shows only active and inactive users of the Outlook Integration query system. – Non-Outlook Integration Users – Shows all users except Outlook Integration Users. – Admin Users – Shows only system administrator users. <i>Note:</i> Name of the Users panel reflects selection (see Managing user accounts, on page 3-14). • Look and Feel – Determines appearance of the PAM window. Choices are: Metal, Motif, and Windows.
View menu	Database Statistics – Displays the PAM Database Statistics Summary panel, which shows number of users, repositories, ACLS, routing rules, and billing groups in the system.
Help menu	<p>About – Shows current version of PAM.</p> <p>PAM Help – Opens PAM's online help in a browser window.</p>
Search button	<p>Used to list only objects that have names starting with text entered in the Search box. (Panels are described later in this table.) For example, in the Users panel, search for ja to find users jadams, jackdoe, and janedoe.</p> <p>When the Domain box is available, the search is limited to names in selected domain.</p>
Domain	<p>Domain for which simple routing rules and filters are displayed. Select domain from the pull-down list. Selection limits scope of the Search and A-to-Z filter buttons.</p> <p>(Domain is available only when the current panel is Simple Routing Rules or Routing Filters.)</p>
All button	Used to list all objects of type indicated by panel (tab) name.

Table 3-1: Platform Account Manager window features (continued)

Feature	Description
A-to-Z buttons	Used to show only names starting with button letter. Names correspond to objects of current panel. (Panels are described later in this table.) When the Domain box is available, names are limited to those in selected domain. (These buttons are not available in the Routing Filters panel.)
scroll bar	Slide the scroll bar to display left or right side of the PAM window.
panels	<p>Click a tab to view corresponding panel for object. All panels have the following parts:</p> <ul style="list-style-type: none"> • List of (up to 50) objects filtered by Search, Domain, and A-to-Z selections. • Information about object selected in the list. • Apply button: Saves changes made to displayed information. • Reset button: Clears changes made (prior to clicking Apply) and redisplay current database information. <p>Individual panels display the following objects:</p> <ul style="list-style-type: none"> • Users (see Managing user accounts, on page 3-14) – RISS users of the kind determined by Options > Show Users. You can create and delete users, view and edit user information, and change user status and privileges. • Repositories (see Managing repositories, on page 3-19) – RISS repositories. You can create repositories and add, view, or delete repository access control lists. You cannot delete existing repositories. • ACLs (see Managing access control lists (ACLs), on page 3-23) – Access control lists. You can create and delete ACLs, and add or remove users in existing ACLs. • Routing Rules (see Managing routing filters, on page 3-34) – You can create, view, edit, and delete routing rules and associate them with repositories. • Simple Routing Rules (see Managing simple routing rules, on page 3-31) – You can create, view, edit, and delete simple routing rules and associate them with repositories. • Routing Filters (see Managing routing filters, on page 3-34) – You can create, view, edit, and delete routing filters and associate them with repositories.

Table 3-1: Platform Account Manager window features (continued)

Feature	Description
navigation buttons	<p>Shows number of qualified objects displayed. For example, 1-50 of 230 means the first 50 objects are shown and a total of 230 objects match selected type and filter criteria.</p> <p>Click navigation buttons to:</p> <ul style="list-style-type: none">• < – Display previous 50 qualified objects.• << – Display 50 qualified objects before previous 50.• > – Display next 50 qualified objects.• >> – Display 50 qualified objects after next 50.• New – Display the Add New Item dialog box, which is specific to the current panel (see previous panel descriptions). You can create new objects.• Delete – Delete selected object. (Not available in all views.)
connection status	<p>How long it took PAM to connect to database. Example: Status: Connected in 0 minutes 17 seconds.</p>
feedback	<p>Status of last action. Example: Updated user: bbrown.</p>

Performing basic PAM tasks

Use the Platform Account Manager window to create, view, modify, or delete objects, such as user accounts, ACLs, or routing rules.

For a sample scenario, see [Example: Integrating new department, on page 3-39](#). For detailed information about individual PAM panels, see panel descriptions later in this chapter.

Creating PAM objects

1. Click the object tab, (for example, ACLS).
2. Click New. The Add New Item dialog box appears.
3. Define the object.
4. Click Add.

Viewing PAM objects

1. Click the object tab (for example, click Repositories).

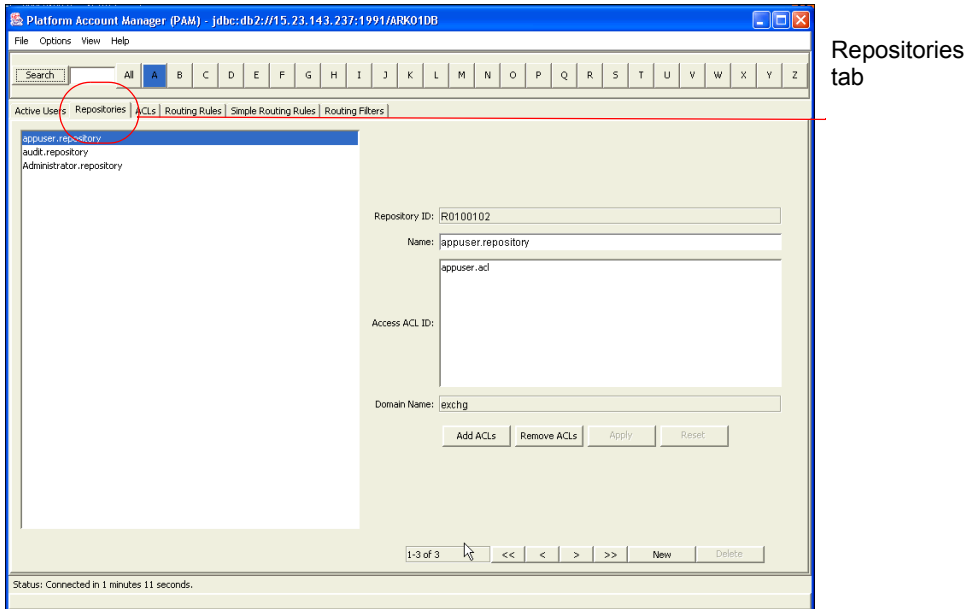


Figure 3-2: Repositories tab

2. Use the Search, A-to-Z, <, <<, >, and >> buttons to display target object in the list.
3. Select target object in the list.
4. To modify selected object, do one or more of the following, and click Apply.

- Change values in editable parts of the panel.
- If selected object is a collection of other objects:

To add or remove member objects in the collection, use the Add *<object type>* or Remove *<object type>* button, respectively. See [Adding member objects to collection objects, on page 3-12](#), for instructions.

(The following object types are **collections**: repositories, ACLs, simple routing rules, and routing filters.)

5. To delete selected object, click Delete, and click Yes in confirmation message.

Modifying PAM objects

1. Click the object tab (for example, click Repositories).
2. Use the Search, A-to-Z, <, <<, >, and >> buttons to display target object in the list.
3. Select target object in the list.
4. To modify selected object, do one or more of the following, and click Apply.
 - Change values in editable parts of the panel.
 - If selected object is a collection of other objects:

To add or remove member objects in collection, use the Add <object type> or Remove <object type> button, respectively. See [Adding member objects to collection objects, on page 3-12](#), for instructions.

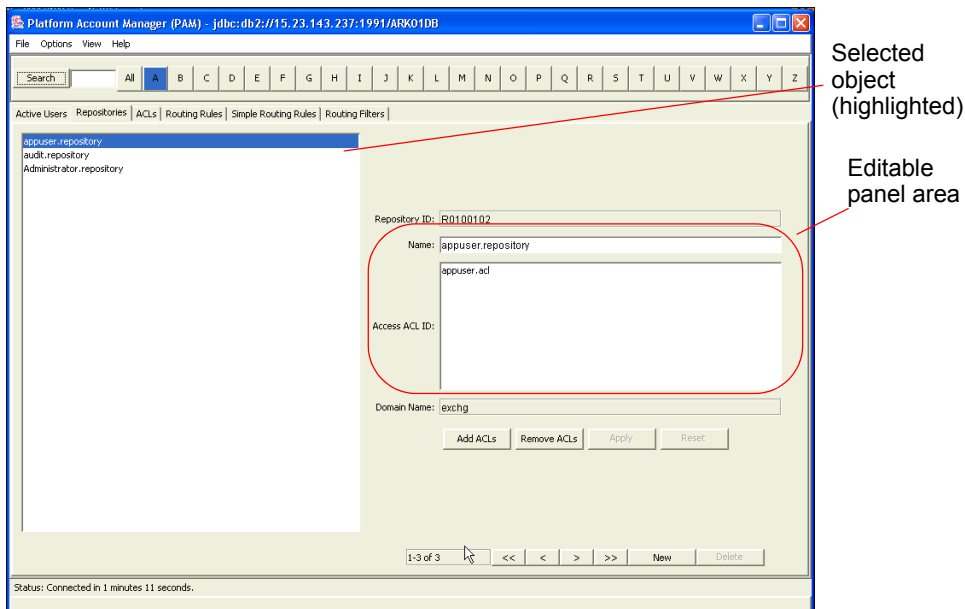


Figure 3-3: Modify repositories object

The following object types are **collections**: repositories, ACLs, simple routing rules, and routing filters.

5. To delete selected object, click Delete, and click Yes in confirmation message.

Deleting PAM objects

1. Click the object tab (for example, click Active Users).
2. Use the Search, A-to-Z, <, <<, >, and >> buttons to display target object in the list.
3. Select target object in the list.
4. To delete selected object, click Delete, and click Yes in confirmation message.

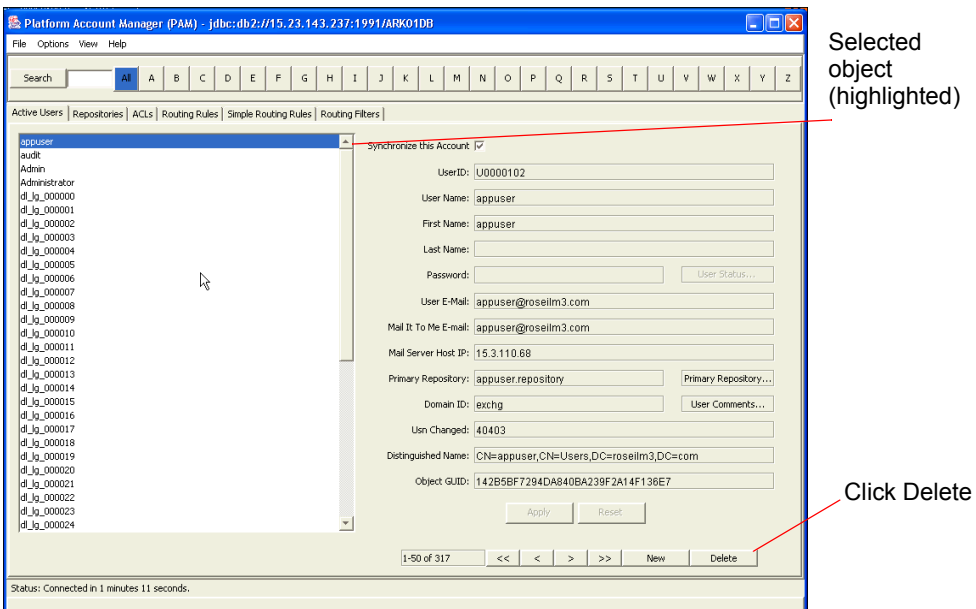


Figure 3-4: Delete Object

Adding member objects to collection objects

These procedures assume you selected the collection object in the list at the left of the PAM window. See [Viewing PAM objects, on page 3-8](#), for instructions.

1. Click Add <type>. (The object <type> depends on the current panel.) The Select <type> dialog box appears.

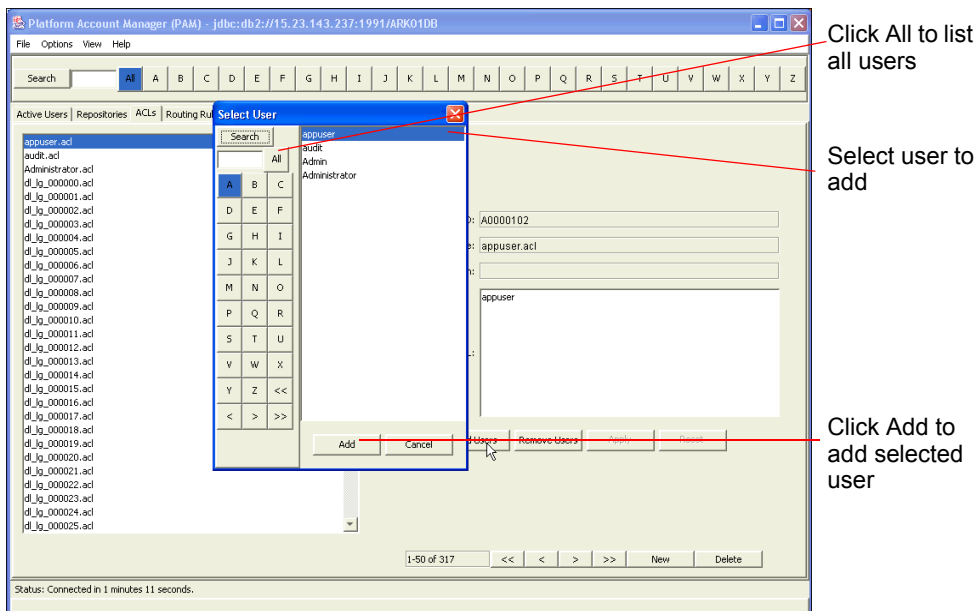


Figure 3-5: Select User dialog box

2. Select object to add to collection. (Use the Search, All, A-to-Z, <, <<, >, and >> buttons to navigate the list.)
3. Click Add.
4. Click Apply.

Example: To add user to ACL

1. Select ACL in the ACLs panel.
2. Click Add User.

3. Select user in the Select User dialog box.
4. Click Add in the Select User dialog box.
5. Click Apply in the ACLs panel.

Removing member objects from collection objects

These procedures assume you selected the collection object in the list at the left of the PAM window. See [Viewing PAM objects, on page 3-8](#), for instructions.

1. Select object in the list.
2. Click Remove *<type>*. (The object *<type>* depends on the current panel.) A confirmation message appears
3. Click Yes.
4. Click Apply.

Example: To remove user from ACL

1. Select ACL in list at the left of the ACLs panel.
2. Select user in the box User entries for this ACL.
3. Click Remove User in the ACLs panel, and confirm (Yes).
4. Click Apply in the ACLs panel.

Managing user accounts

Use the Users panel to view or change individual user accounts on RISS. Choose set of users to view with Options > Show Users. See Options menu in Table 3-1. The panel name (on the tab) changes accordingly.

For example, if you choose Options > Show Users > Active Users, the panel heading is Active Users, and you can view only active users (those able to log in to the system).

Regardless of selected set of users, you can create or delete user accounts, or change privileges and identifying information for a given user.

Accessing Users panel

Click the Users tab.

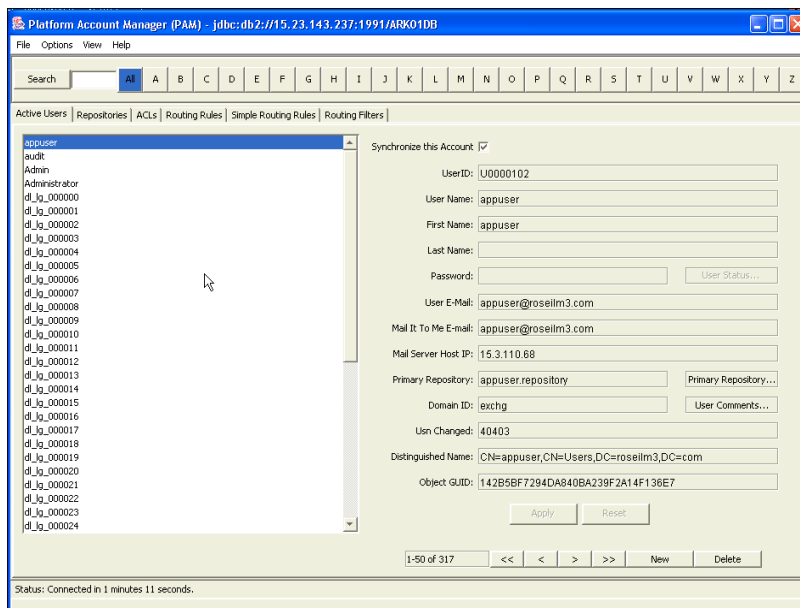


Figure 3-6: Users panel

Table 3-2: Users panel, PAM window

Feature	Description
object list	Users on this system determined by Options > Show Users, and indicated by current panel name. (See Filtering list of users, on page 3-16.)
Synchronize this Account	If DAS is allowed to update selected user account. See Viewing non-editable user information, on page 3-16.
UserID	Automatically generated identifier for selected user; unique to the system. (Not editable.)
User Name	(Required.) System login name for selected user.
First Name	First name of selected user.
Last Name	Last name of selected user.
Password	Login password for selected user.
User Status	Displays user profile options. See Modifying email information, on page 3-17.
User E-Mail	Email address for selected user.
Mail It To Me E-mail	(Required.) Email destination when selected user clicks Mail It To Me for an archived document.
Mail Server Host IP	IP address of mail server for selected user. (Optional, unless querying within Microsoft Outlook is required.)
Primary Repository	ID of repository created with selected user. (Not editable. Users can be given access to additional repositories through ACLs.)
Domain ID	Domain to which selected user belongs. (Not editable. Value is supplied when account is created.)
User Comments	Displays administrators' comments on selected user account.
Usn Changed	USN imported from corresponding user account on LDAP server the last time DAS ran. (Not editable.) DAS uses this number to detect updates to the account (see Viewing non-editable user information, on page 3-16.).
Distinguished Name	Corresponding object name, relative location in LDAP tree, and domain. CN (Common Name) is object name, cn is its branch in the tree, and dc values are domain names. (Not editable.) DAS supplies this value.

Table 3-2: Users panel, PAM window (continued)

Feature	Description
Object GUID	Globally Unique Identifier of corresponding user account on LDAP server. (Not editable.) This is DAS' key to correct account on LDAP server.
Apply button	Used to save changes made to editable fields. Button is unavailable until you change a value.
Reset button	Used to clear unsaved changes and redisplay last saved values. Button is unavailable until you change a value.
New button (specifics)	Used to add new users. New users are automatically assigned active status, so they can log into the system.

Filtering list of users

Choose set of users to view with Options > Show Users. See Options menu in Table 3-1. The panel name (on the tab) changes accordingly. For example, if you choose Options > Show Users > Active Users, the panel heading is Active Users, and you can view only active users (those able to log in to the system).

Only the first 50 items in the list are shown. To filter the list, use the Search and A-to-Z buttons.

Regardless of selected set of users, you can create or delete user accounts, or change privileges and identifying information for a given user.

Viewing non-editable user information

Select Synchronize this Account if you want DAS to update the selected user account. If selected, the User Name, First Name, Last Name, User E-Mail, Mail It To Me E-mail, Mail Server Host IP, and User Status fields cannot be edited. They are synchronized with values on the LDAP server.

Adding new users

Choose set of users to view with Options > Show Users. These instructions specify actions for the Active Users selection.

1. Click the Active Users tab.
2. Click New. The Add New Item dialog box appears.
3. Choose domain for new user and enter name, email, and host information. You cannot select user status or enter comments.
4. After closing the Add New Item dialog box, use the Create User Options dialog box to choose one or both of the following:
 - a. Add Repository, ACL & Simple Routing Rule – If selected (the default), an individual repository is created for the user with a new ACL, giving user access to the repository, and a new simple routing rule that routes all email to and from the user to the repository. The repository and ACL have the same name as the user. The user email address is also the name of the simple routing rule.
 - b. Add the following Routing Rule – When enabled, a routing rule is automatically created, defined by text entered in the accompanying field.

Note: See [Creating marketing department users, on page 3-41](#), for an example of creating a user.

Modifying email information

1. Click User Status.
2. Select Active User if user has a current login.
3. Select Outlook Initialized if user is using RISS through Microsoft Outlook.
4. Select Administrative Privileges if user is allowed to perform administrative tasks, such as using PCC and PAM.
5. Select BCC User if user is allowed to view blind carbon copy addressees of mail in the user's repositories.

6. If you change selected options, click Apply. Otherwise, click Cancel to close the User Status dialog box.

Note: The User Status button is unavailable if Synchronize this Account is selected.

Viewing and modifying user comments

1. Click User Comments.
2. In the Comment dialog box, click Update.
3. Type new comments in the Input dialog box, and click OK. The new comment replaces the previous comment.
4. Click OK. The Input dialog box closes.

Managing repositories

Use the Repositories panel to view, add, or change RISS repositories. You can change which ACLs apply to a given repository. You cannot delete a repository.

Accessing Repositories panel

Click the Repositories tab.

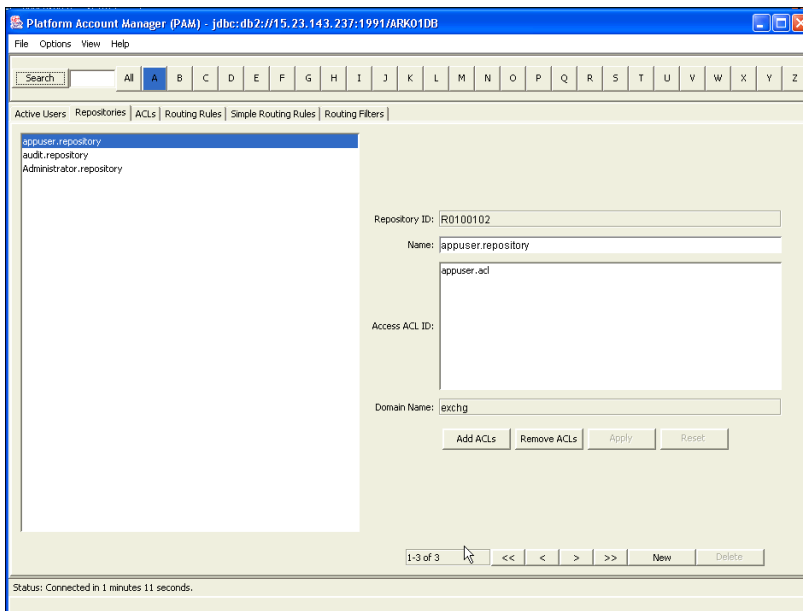


Figure 3-7: Repositories panel

Table 3-3: Repositories panel, PAM window

Feature	Description
object list	Repositories on system.
Repository ID	Automatically generated identifier for selected repository. Number is unique to the system. (Not editable.)
Name	(Required.) Name of selected repository.

Table 3-3: Repositories panel, PAM window (continued)

Feature	Description
Access ACL ID	ACLs defined for selected repository.
Domain Name	Domain to which selected repository belongs. (Value is supplied when repository is created. See User Management view (Dynamic Account Synchronization) , on page 2-28, for DAS configuration.)
Add ACLs button	Used to add ACL to repository. See Adding ACLs to repositories , on page 3-22.
Remove ACLs button	Used to remove ACL from repository. See Removing ACLs from repositories , on page 3-22.
Apply button	Used to save changes made to editable fields. Button is unavailable until you change a value.
Reset button	Used to clear unsaved changes and redisplay last saved values. Button is unavailable until you change a value.
New button (specifics)	Used to add repository. See Adding repositories , on page 3-21.

Filtering list of repositories

The object list displays a list of repositories on this system. Only the first 50 items in the list are shown, and the list can be filtered using the Search and A-to-Z buttons. (See [Filtering list of users](#), on page 3-16.)

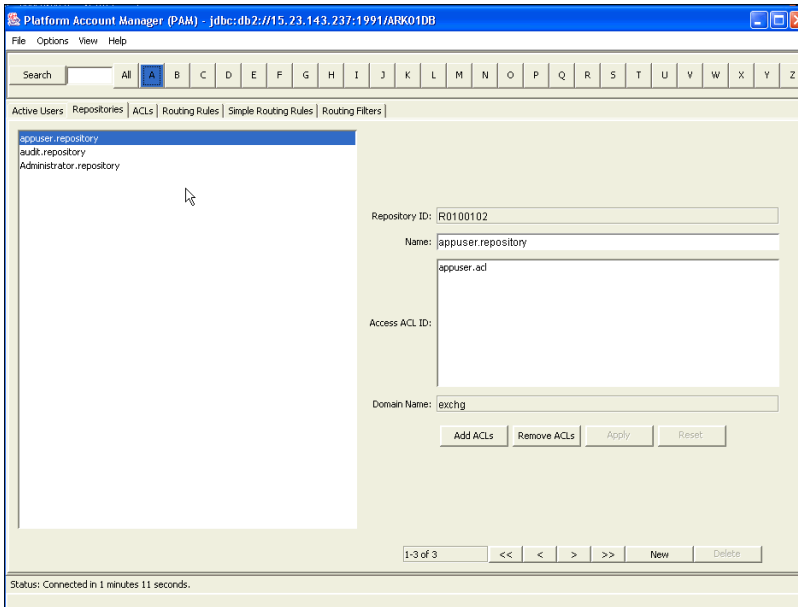


Figure 3-8: Filter repositories

Viewing non-editable repository information

Under the Access ACL ID feature, double-click an ACL entry to display the ACL dialog box, where you can view (but not modify) the ACL definition. The ACL dialog box provides the same information as the ACLs panel for that ACL. See [Managing access control lists \(ACLs\), on page 3-23](#).

Adding repositories

1. Click New. The Add New Item dialog box appears.
2. Define repository name, choose its domain, and choose ACLs for the new repository.

Note: See [Creating repository for marketing department, on page 3-42](#), for an example.

Adding ACLs to repositories

1. Select repository from the object list.
2. Click Add ACLs.
3. Click to display the Select ACL Entries dialog box, where you can select access control lists and add them to selected repository.
4. Click Apply in the Repositories panel.

Removing ACLs from repositories

1. Select repository from the object list.
2. Click Remove ACLs.
3. Select Access ACL ID entry, and click Remove ACLs.
4. Click Apply.

Managing access control lists (ACLs)

Use the ACLs panel to create or delete an access control list, or change users in a given ACL.

Accessing ACLs panel

Click the ACLs tab.

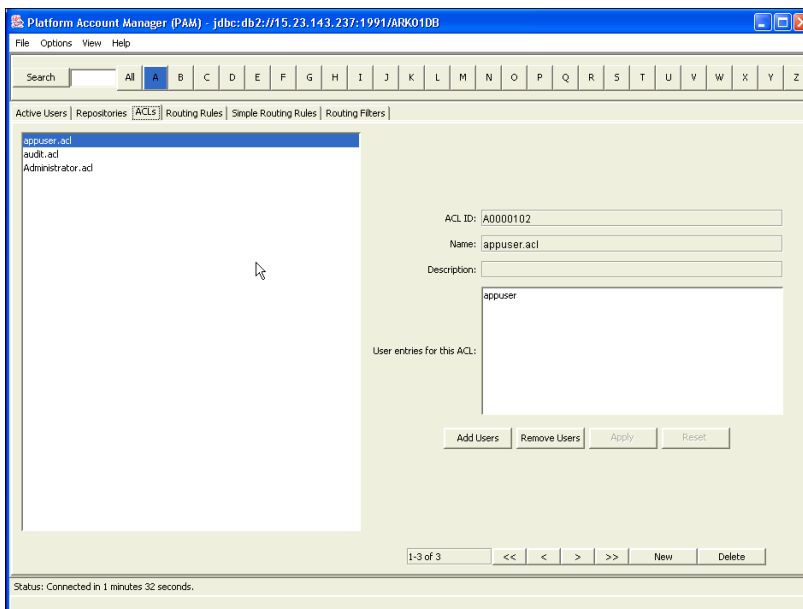


Figure 3-9: ACLs panel

Table 3-4: ACLs panel, PAM window

Feature	Description
object list	Access control lists on the system. See Filtering list of ACLs, on page 3-24 .
ACL ID	Automatically generated identifier for selected ACL. Value is unique to the system. (Not editable.)

Table 3-4: ACLs panel, PAM window (continued)

Feature	Description
Name	(Required.) Name of selected ACL. See Viewing non-editable ACL information, on page 3-24 .
Description	Description of selected ACL. See Viewing non-editable ACL information, on page 3-24 .
User Entries for this ACL	List of user names in selected ACL. See Viewing user profiles, on page 3-26 .
Add User button	Used to add users to selected ACL. See Adding users to ACLs, on page 3-25 .
Remove User button	Used to remove user from selected ACL. See Removing users from ACLs, on page 3-25 .
Apply button	Used to save changes made to editable fields. Button is unavailable until you change a value.
Reset button	Used to clear unsaved changes and redisplay last saved values. Button is unavailable until you change a value.
New button (specifics)	Used to create ACLs. See Adding ACLs, on page 3-25 .

Filtering list of ACLs

The object list displays access control lists on this system. Only the first 50 items in the list are shown. To filter the list, use the Search and A-to-Z buttons. (See [Performing basic PAM tasks, on page 3-8](#).)

Viewing non-editable ACL information

The Name feature displays the non-editable name of selected ACLs. The value is supplied when ACL is created. See [User Management view \(Dynamic Account Synchronization\), on page 2-28](#), for DAS information.

The Description feature displays the non-editable description of selected ACL. The value is supplied when ACL is created.

Adding ACLs

1. Click New. The Add New Item dialog box appears.
2. Type ACL name in the ACL Name field.
3. Type ACL description in the Description field.
4. Choose user entries for ACL.

Note: See [Creating ACL for managers to access marketing email, on page 3-42](#), for an example.

Adding users to ACLs

1. Click Add User. The Select User dialog box appears.
2. Select one or more users.
3. Click Add.
4. Click Apply in the ACLs panel.

Note: See [Adding member objects to collection objects, on page 3-12](#), for an example.

Removing users from ACLs

1. Select a user in the User Entries for the ACL list.
2. Click Remove User. A confirmation dialog appears.
3. Click Yes.
4. Click Apply in the ACLS panel.

Note: See [Removing member objects from collection objects, on page 3-13](#), for an example.

Viewing user profiles

Under the User Entries for ACL feature, double-click an entry to display the User dialog box, where you can view (but not modify) the user profile. The User dialog box provides the same information as the Users panel for that user. See [Managing user accounts, on page 3-14](#).

Managing routing rules

Use the Routing Rules panel of the PAM window to create, edit, or delete routing rules, or choose the repository associated with a rule.

Note: Use simple routing rules (see [Managing simple routing rules, on page 3-31](#)) instead of the Routing Rules panel whenever possible. Extensive use of rules can negatively impact system performance.

Accessing Routing Rules panel

Click the Routing Rules tab.

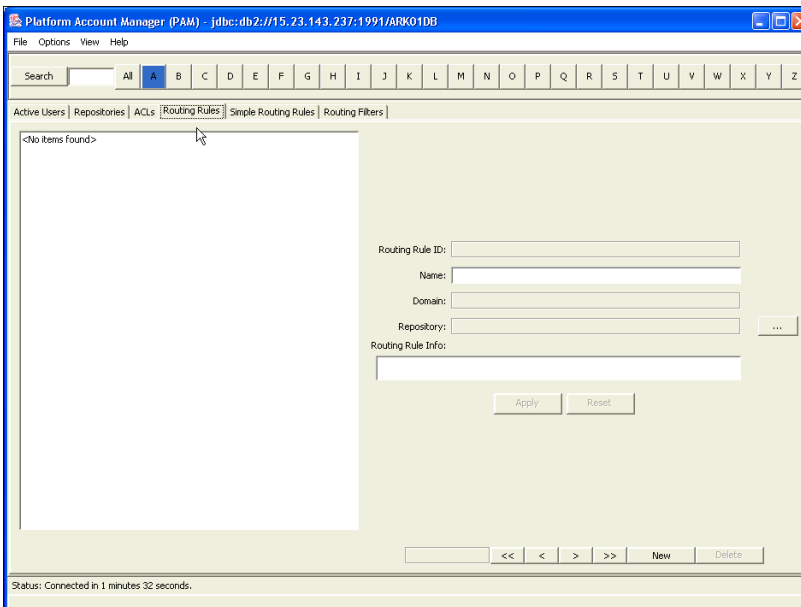


Figure 3-10: Routing Rules panel

Table 3-5: Routing Rules panel, PAM window

Feature	Description
candidate objects	List of all routing rules. See Filtering list of routing rules, on page 3-28 .
Routing Rule ID	Automatically generated identifier for selected routing rule. See Viewing non-editable routing rule information, on page 3-28 .
Name	(Required.) Name of selected routing rule.
Domain	Domain of selected routing rule. See Viewing non-editable routing rule information, on page 3-28 .
Repository	Repository routing rule applies to. Emails matching the rule are routed to this Repository.
...	Used choose destination repository. See Adding repositories to routing rules, on page 3-30 .
Routing Rule Info	Definition of routing rule. See Defining routing rule information, on page 3-29 .
New button (specifics)	Used to create routing rules. See Adding routing rules, on page 3-29 .

Filtering list of routing rules

Click candidate objects to see a list of all routing rules. Only the first 50 items in the list are shown. To filter the list, use the Search and A-to-Z buttons. (See [Performing basic PAM tasks, on page 3-8](#).)

Viewing non-editable routing rule information

Click Routing Rule ID to see automatically generated identifier for selected routing rule. The value is unique to the system, and is not editable.

Click Domain to see domain of selected routing rule. The value is supplied when you create the rule using the New button, and is not editable.

Adding routing rules

1. Click New. The Add New Item dialog box appears.
2. Define rule name.
3. Choose domain.
4. Choose repositories for new routing rule.
5. Define the Routing Rule Info. See [Defining routing rule information, on page 3-29](#).
6. Click Add.

Defining routing rule information

Note: Matching is *not* case-sensitive (b matches B and b), except for Subject field.

Follow these syntax rules when creating a routing rule:

- Each match string is composed of ISO 8859-1 (Latin-1) characters enclosed in double quotes (").
- Each match component includes a keyword followed by an equal sign (=) and a match string. Example: TO="w@z.org".
- Keywords for match components:
 - TO component matches email recipient fields (To, Cc, Bcc, Apparently-To).
 - FROM component matches email sender field (From).
 - Subject component matches any string in the email's Subject field. Example: Subject="meeting" matches Subject: What time is today's Meeting?. Matching of Subject field is case-sensitive: (b matches b, but not B; B matches B, but not b).
 - MessageDateRange component checks when an email was *sent*; it matches if the email's Date field is within the indicated range. Match string is "<date1> TO <date2>", where each date has the syntax of an

email Date field (date, local time, local offset from GMT). Example: MessageDateRange="2003-7-1 00:00 +0700 TO 2003-8-1 00:00 +0700".

- Email addresses are used as match strings for TO and FROM. Each must respect standard email address syntax. Each is matched completely. Example: TO="c@b.com" matches c@b.com, but *not* abc@b.com.
- Parentheses ((,)) are used for grouping. Example: (FROM="a@b.com" OR (TO="w@z.org" AND Subject="meeting")).

Modifying routing rules

1. Select a routing rule in the object list.
2. Change values in the following fields:
 - Name
 - Repository
 - Routing Rule Info
3. Click Apply.

Deleting routing rules

1. Select a routing rule in the object list.
2. Click Delete, and click Yes in confirmation message.

Adding repositories to routing rules

Click the ... (ellipsis) button to display the Select Repository dialog box, where you choose the destination repository.

Managing simple routing rules

Use the Simple Routing Rules panel to create, edit, or delete simple routing rules, or choose the repository associated with a rule.

Note: Use simple routing rules instead of the Routing Rules panel (see [Managing routing rules, on page 3-27](#)) whenever possible. Extensive use of rules can negatively impact system performance.

Accessing Simple Routing Rules panel

Click the Simple Routing Rules tab.

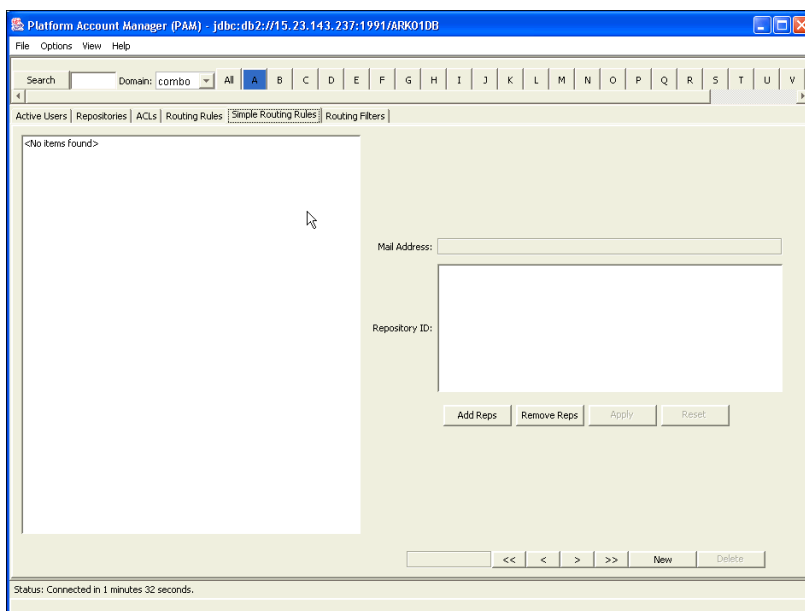


Figure 3-11: Simple Routing Rules panel

Table 3-6: Simple Routing Rules panel, PAM window

Feature	Description
candidate objects	List of all simple routing rules for selected domain. See Filtering list of simple routing rules, on page 3-32 .
Mail Address	(Required.) Mailing address of selected simple routing rule. See Viewing non-editable simple routing rule information, on page 3-32 .
Repository ID	(Required.) List of repositories simple routing rule applies to. See Viewing non-editable simple routing rule information, on page 3-32 .
Add Rep button	Used to add repository to selected simple routing rule. See Adding repositories to simple routing rules, on page 3-33 .
Remove Reps button	Used to remove repository from selected simple routing rule. See Removing repositories from simple routing rules, on page 3-33 .
New button (specifics)	Used to add simple routing rules. See Adding simple routing rules, on page 3-33 .

Filtering list of simple routing rules

Click candidate objects to see a list of all simple routing rules for selected domain. Only the first 50 items in the list are shown. To filter the list, use the Search and A-to-Z buttons. (See [Performing basic PAM tasks, on page 3-8](#).)

Viewing non-editable simple routing rule information

Click Mail Address to see the mailing address of selected simple routing rule. This information is not editable here. Supply this value with the New button. The Mail Address is matched against both sender and recipient addresses. It corresponds to Routing Rule Info (TO= . . . OR FROM= . . .) for a routing rule. See [Managing routing filters, on page 3-34](#).

Click Repository IDs to see a list of repositories to which this simple routing rule applies. Emails matching the rule are routed to each of these repositories. Double-click a repository ID to display the Repository dialog box, where you can view (but not modify) the definition of that repository. (The Repository dialog box provides the same information as the Repositories panel for that repository. See [Managing repositories, on page 3-19](#).)

Adding simple routing rules

1. Click New. The Add New Item dialog box appears.
2. Define the Mail Address.
3. Choose applicable repositories.

Note: For a simple routing rule to have any effect, there must be a routing filter with the same email domain as in the routing rule Mail Address. When you create a simple routing rule, check the Routing Filters panel for a filter with the corresponding domain. If there is no such filter, create one. See [Managing routing filters, on page 3-34](#).

Adding repositories to simple routing rules

1. Click Add Rep. The Select Repository dialog box appears.
2. Add one or more repositories.
3. Click Apply in the Simple Routing Rules panel.

Note: See [Editing simple routing rules for marketing email, on page 3-43](#), for an example.

Removing repositories from simple routing rules

1. Select repository in the Repository ID list, and click Remove Reps.
2. Click Apply in the Simple Routing Rules panel.

Managing routing filters

Use the Routing Filters panel to create, edit, or delete routing filters, or choose the repositories associated with a routing filter.

A **routing filter** checks email domains appearing in all addresses of each email. For each domain in an email matching the Email Domain of a routing filter, the following occurs:

- All simple routing rules with that domain are checked against the email. Simple routing rules matching the email are applied (routing email to repositories associated with the rules).
- Email is routed to repository (Repository ID) defined for the filter—provided the filter's Repository ID does *not* include the special value R0000000 Catchall Repository.

This means a routing filter has two possible uses, based on which domains appear in email addresses:

- Filtering emails before simple routing rules try to match them: only rules with the correct email domains are tried.
- Routing emails from a specific domain to a specific repository. (In this case, it is typically used to associate an audit repository with an email domain.)

After filtering, each email is always checked against routing rules. This is true regardless of the filtering result (possible routing by simple rules and/or filter).

R0000000 Catchall Repository

The special R0000000 Catchall Repository value is an exception. A filter with this value in the Repository ID does *not* route email to the catch-all repository. It does *not*, itself, route email to any repository; rather, it serves only as a filter before checking simple routing rules.

To create a routing filter with the special R0000000 Catchall Repository value, choose Catchall Repository in the Select Repository dialog box – see below. Do this to filter email before checking simple routing rules, without also routing email directly to a repository based on email domain.

Note: Before you add a repository to a filter Repository ID field already containing the special value R0000000 Catchall Repository, remove the entry R0000000 Catchall Repository. A routing filter with R0000000 Catchall Repository must *not* contain any other Repository ID values.

Routing filter examples

Table 3-7 shows what happens when emails with various addresses are filtered using different values for Repository ID. The Email Domain of each filter is the same in all examples: ourcorp.com. (Each example shows a single email, with multiple addresses.)

Table 3-7: Routing filter examples

Repository ID	Addresses in email	Actions
marketingstore	johndoe@ourcorp.com, janechoi@ourcorp.com, june@other.com	<ul style="list-style-type: none"> • Check for simple routing rules matching johndoe@ourcorp.com and janechoi@ourcorp.com. • Route email to marketingstore. • Check for matching routing rules.
R0000000 Catchall Repository	johndoe@ourcorp.com, janechoi@ourcorp.com, june@other.com	<ul style="list-style-type: none"> • Check for simple routing rules matching johndoe@ourcorp.com and janechoi@ourcorp.com. • Check for matching routing rules.
<any>	june@other.com, johndoe@another.com	Check for matching routing rules.

Accessing Routing Filters panel

Click the Routing Filters tab.

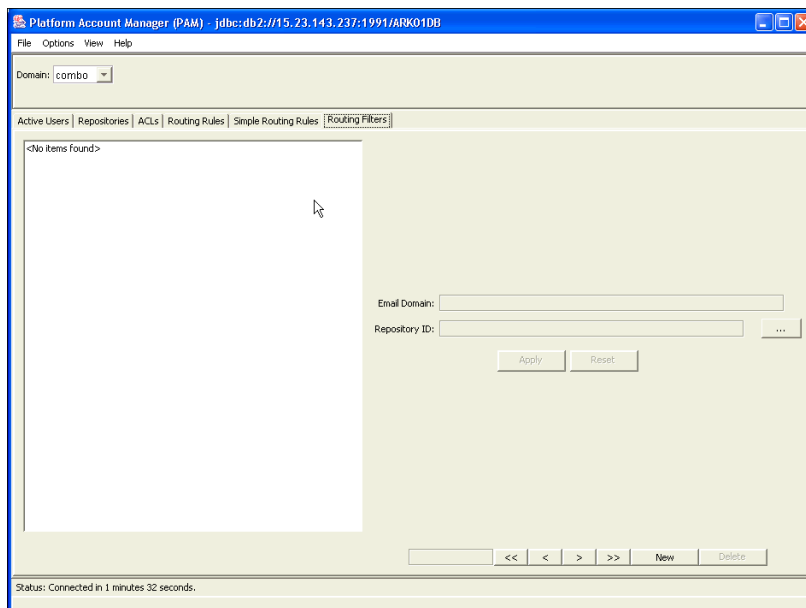


Figure 3-12: Routing Filters panel

Table 3-8: Routing Filters panel, PAM window

Feature	Description
candidate objects	List of routing filters for selected domain. See Filtering list of routing rules, on page 3-37 .
Email Domain	(Required.) Email domain of selected routing filter (example: mycorp.com). Filter applies to all emails with this domain in the mail header. (Not editable. Value is supplied when filter is created.)
Repository ID	(Required.) Repository to which emails from the Email Domain are routed (in addition to users' repositories) unless the R0000000 Catchall Repository is specified – see <i>Note</i> , above.

Table 3-8: Routing Filters panel, PAM window (continued)

Feature	Description
...	Used to display the Select Repository dialog box, where you can add a repository to selected routing filter. The new repository replaces the previous repository in the Routing Filters panel. You must click Apply in the Routing Filters panel for the addition to take effect. Before adding a repository, ensure that R0000000 Catchall Repository is <i>not</i> a Repository ID – see <i>Note</i> , above.
Apply button	Used to save changes made to editable fields. Button is unavailable until you change a value.
Reset button	Used to clear unsaved changes and redisplay last saved values.
New button (specifics)	Used to add routing filter. See Adding routing filters, on page 3-37 .

See Also

- [Managing simple routing rules, on page 3-31](#).
- [Managing routing rules, on page 3-27](#), for information on routing rules.

Filtering list of routing rules

Click candidate objects to see a list of routing filters for selected domain. Only the first 50 items in the list are shown. To filter the list, use the Search and A-to-Z buttons. (See [Performing basic PAM tasks, on page 3-8](#).)

Adding routing filters

1. Click **New**. The **Add New Item** dialog box appears.
2. Define the Email Domain.
3. Choose domain of application for new routing filter.
4. Click ... to choose applicable repositories.
5. Click **Add**.

Modifying routing filters

1. Select a routing filter in the object list.
2. Change values in the Email Domain or Repository ID fields.
3. Click Apply.

Deleting routing filters

1. Select a routing filter in the object list.
2. Click Delete, and click Yes in confirmation message.

Example: Integrating new department

Problem statement and solution

Problem

In this example scenario, your company, OurCorp, is splitting the marketing function from the Sales Department to create a separate Marketing Department. The current marketing person, Mark Marcom, is becoming the manager of the Marketing Department, and two new marketing employees, John Doe and Jane Choi, are being hired.

You must integrate the new Marketing department into the RISS archiving and retrieval system.

Solution

One way to accomplish this is as follows:

1. Create a single repository, `marketingstore`, for all email to and from Marketing Department personnel (John, Jane, and Mark). Use the Repositories panel to do this. See [Creating repository for marketing department, on page 3-42](#), for instructions.
2. Create an ACL to access (query) the `marketingstore` repository. Only Mark, the Marketing Department manager, and Betty Bigboss, the company CEO, will belong to this ACL, since it will enable them to see all email to and from John, Jane, and Mark. Use the ACLs panel to do this. See [Creating ACL for managers to access marketing email, on page 3-42](#), for instructions.

Because you must select one or more existing ACLs when you create a repository, you must create the marketing ACL before the repository.

3. Create users `johndoe` and `janechoi` for the new employees John and Jane. Use the Users panel to do this. See [Creating marketing department users, on page 3-41](#), for instructions.

Creating these users will also automatically accomplish the following (provided the option ACL & Simple Routing Rule is enabled in the Create User Options dialog box—the default value):

- Create individual repositories for John’s email and Jane’s email.
- Create access control lists (ACLs) for John and Jane to access (query) their respective individual repositories.
- Create simple routing rules to route John’s email and Jane’s email to their respective individual repositories.

The new repositories and ACLs are named the same as the users (johndoe and janechoi). The new simple routing rules are named with the user email addresses (johndoe@ourcorp.com and janechoi@ourcorp.com).

4. Edit the simple routing rules for members of the Marketing Department (Mark, John, and Jane) to route their individual incoming and outgoing email to the marketingstore repository (in addition to routing it to their own repositories). Use the Simple Routing Rules panel to do this. See [Editing simple routing rules for marketing email](#), on page 3-43, for instructions.

See Also

- [Managing user accounts](#), on page 3-14
- [Managing repositories](#), on page 3-19
- [Managing access control lists \(ACLs\)](#), on page 3-23
- [Managing simple routing rules](#), on page 3-31

Alternative solutions

There are of course alternative ways to add a new department and new users, with the appropriate email routing and query access. For example, instead of creating a separate marketing ACL for the marketing repository, you could add the individual manager ACLs (Mark’s and Betty’s) to the marketing repository. Or you could dispense with the marketing ACL and marketing repository by adding Mark and Betty to the ACLs for John’s and Jane’s individual repositories.

The relationships between users, repositories, ACLs, and simple routing rules are all *N-to-M*: any number of users can be associated with any number of repositories, and so on. How you organize these entities and relationships is up to you, but choose a scheme and stick to it.

For ease in maintenance and flexibility in access control, using abstract collection objects like a marketing repository and a marketing ACL can be advantageous. Trying to manage everything at the fine-grain level of individual users and their relationships to user repositories can lead to extra work for both system administrators and end users.

For example, with a Marketing Department repository, a manager can limit a query to search only Marketing Department email.

Creating marketing department users

Use the Users panel to create active users for John and Jane. (It does not matter which kind of users are currently displayed in the Users panel.) Do the following once for John and once for Jane:

1. Click the Users tab.
2. Click New. The Add New Item dialog box appears.
3. Enter the following:
 - User Name – For John, johndoe; for Jane, janechoi.
 - First Name (John; Jane) and Last Name (Doe; Choi)
 - Leave the Password blank. John and Jane will set their own passwords after they log in to the query system.
 - User E-Mail and Mail It To Me E-Mail – johndoe@ourcorp.com and janechoi@ourcorp.com (use same addresses for each field).
 - Mail Server Host IP – Mail server IP for the company Ourcorp is 192.168.10.3.
 - Domain ID – Choose email domain ourcorp.com from the pull-down list of existing domains for your company.
4. Click Add. The Create User Options dialog box appears. Click OK, without changing default values.

When enabled (the default), the option ACL & Simple Routing Rule automatically creates a repository, ACL, and simple routing rule for the new user. This gives the user access to his/her own repository, where all of his/her incoming and outgoing email is routed.

5. Click Apply in the Users panel (PAM window).

Creating ACL for managers to access marketing email

Use the ACLs panel to give Manager Mark and CEO Betty access to all email to and from members of the Marketing Department.

1. Click the ACLs tab.
2. Click New. The Add New Item dialog box appears.
3. Enter the following:
 - Name – marketingaccess.
 - Description – Access to the Marketing Department repository.
 - User entries for this ACL – Click Add User. Use the Select User dialog box to choose users to add to the ACL: markmarcom and bettybigboss. Click Add in the Select User dialog box.
4. Click Add in the Add New Item dialog box.
5. Click Apply in the ACLs panel (PAM window).

Creating repository for marketing department

Use the Repositories panel to create a repository, marketingstore, for the marketing department.

1. Click the Repositories tab.
2. Click New. The Add New Item dialog box appears.
3. Enter the following:
 - Name – marketingstore.
 - Access ACL ID – Click Add ACL. Use the Select ACL Entries dialog box to choose the ACL to add to the repository: marketingaccess. Click Add in the Select ACL Entries dialog box.
4. Click Add in the Add New Item dialog box.
5. Click Apply in the Repositories panel (PAM window).

Editing simple routing rules for marketing email

Use the Simple Routing Rules panel to add the new Marketing Department repository, *marketingstore*, to the existing simple routing rules for each Marketing Department user (John, Jane, and Mark):

1. Click the Simple Routing Rules tab.
2. Use the A-to-Z buttons or Search button to navigate to the list of candidate objects containing the user's email address.
3. Select the user's email address.
4. Click Add Rep. Use the Select Repository dialog box to add the *marketingstore* repository to the simple routing rule for the user, so email to and from the user is also routed to the Marketing Department repository. Click Add in the Select Repository dialog box.
5. Click Apply in the Simple Routing Rules panel (PAM window).

CHAPTER 4

PST Importer

This chapter contains these topics:

- [PST Importer overview, on page 4-2](#)
- [Installing PST Importer, on page 4-4](#)
- [Using PST Importer, on page 4-6](#)
- [Archive Request file, on page 4-16](#)

PST Importer overview

PST Importer allows system administrators to:

- Load legacy (pre-RISS 1.0) PST files into RISS.
- Scan PST files to ensure RISS finds and archives new messages.
- Provide optional “tombstoning” of messages in PST files.

Note: PST Importer modifies messages by removing attachments and possibly body content. This altered message is referred to as a *tombstone*. You may be more familiar with the term *stub*. Outlook users see a stub icon next to tombstoned messages. PCC screens also use stub to refer to tombstones.

This section discusses these topics:

- [PST Importer process, on page 4-2](#)
- [Archive Request file, on page 4-3](#)

PST Importer process

The following is the PST Importer process:

1. Create or plan to use an existing Archive Request file. To create this file, use Archive Request Loader manually or with a script.
2. Use Archive Request Loader to validate that each file set in the Archive Request file is available and has not been imported. Each validated file is added to `PST.MDB` for processing.
3. Use PST Import Monitor to complete the import process. PST Importer reads the PST file, and selects messages that have not been tombstoned or archived for processing. Also use PST Importer to modify the message by removing the body (depending on content type) and attachments. This saves the message as a tombstone or stub. Tombstoning is optional.

Archive Request file

The Archive Request file defines the set of documents to be archived. Each file requires the following:

- Universal Naming Convention (UNC) path
- Option to distribute emails to all recipients (From, To, Cc, and Bcc)
- Option to tombstone and remove body and/or attachments
- List of user repositories to receive document

These parameters are supplied in an XML file format generated with Archive Request Loader. Otherwise, provide Archive Request Loader with an XML file created by another method. For a description of each tag and a sample XML file, see [Archive Request file, on page 4-16](#).

Installing PST Importer

This section discusses these topics:

- [Installation requirements, on page 4-4](#)
- [Installation procedure, on page 4-5](#)

Installation requirements

Before installing PST Importer, verify you meet the following requirements.

Hardware requirements

- Client machine with 512 MB RAM and 200 MB free disk space

Client software requirements

- Uninstall HP RISS Document Manager *before* installing PST Importer.
- Windows 2000 or later. *Highly recommended:* Windows XP.
- Outlook 2000 or later. *Highly recommended:* Outlook 2003.
- Collaboration Data Objects (CDO) installed.

Note: If you use Outlook 2003, also install Service Pack 1 for the Outlook plug-in to work correctly.

RISS software requirements

- Audit repository that receives log files and status reports
- SMTP access for client machine

Network requirements on client machine

- Access to the RISS HTTP portal without proxy
- Access to Exchange mailbox for Global Address List (GAL) name resolution

- Read/Write access to PST files to be imported
- Access to Outlook and Exchange without logon prompts

Installation procedure

Install PST Importer on a client machine.

1. Verify that client machine meets installation requirements. HP highly recommends using Outlook 2003 on Windows XP. See [Installation requirements, on page 4-4](#).
2. On a client machine, run the `setup.exe` installation file provided by your HP representative.
3. Follow the instructions in the installation wizard, and accept all defaults.

Note: The installation wizard installs Microsoft's .NET Runtime support if necessary.

Using PST Importer

This section explains how to use the PST Importer tools and discusses these topics:

- [Archive Request Loader, on page 4-6](#)
- [PST Import Monitor, on page 4-11](#)

Archive Request Loader

Use Archive Request Loader to create or validate an Archive Request file. This tool also generates an output log file, detailing issues that occurred during the load process.

Before adding a file to PST.MDB, Archive Request Loader performs the following tasks:

- Verifies accessibility to file with appropriate access rights.
- Obtains hash of file to be inserted.
- Queries PST.MDB for duplicate entry using generated hash.
- If not already inserted, queries RISS for duplicate entry.
- If no duplicate entry is found on RISS, proceeds with insertion.

Creating or revising an Archive Request file

To create an Archive Request file, use Archive Request Loader. Use the same procedure to revise a file, which you can then resubmit for subsequent processing.

If you plan to create a file using another method, see [Archive Request file, on page 4-16](#) for a description of the XML tags and a sample XML file.

1. Click Start > Programs > Hewlett-Packard > RISS PST Importer > Archive Request Loader, or enter `<install_path>/HPPSTInit` from the command line. The following window appears.

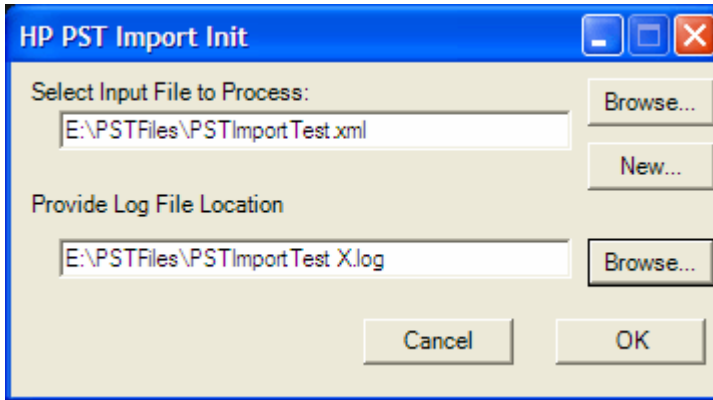


Figure 4-1: Archive Request Loader window

2. Click New. The following window appears.

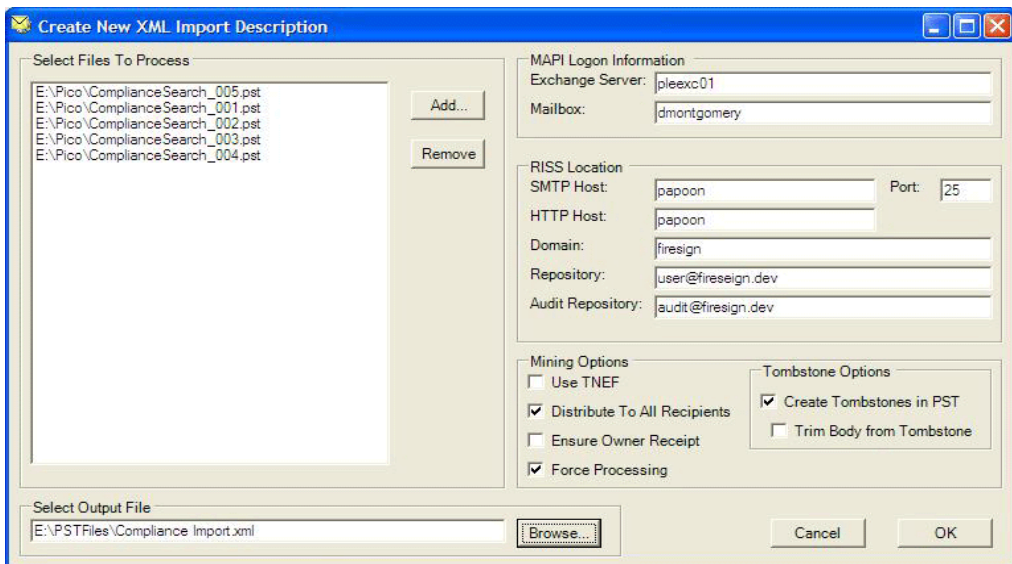


Figure 4-2: Creating a new file

3. Click Add, and select PST files. Only files in the Select Files To Process list are imported. In the file you are creating, corresponding XML tags are `<FileSpecList>` and `<FileSpec>`.

4. To import PST files larger than 150 MB, edit the following setting in `RISS PST Importer.ini` to reduce performance degradation and increase throughput:

[PSTLaunchMgr]

MaxProcesses=1

5. If necessary, select PST files you do not want to process, and click **Remove**.
6. In the **Select Output File** box, enter the path and file name of the file you are creating or revising, or click **Browse** to navigate to a location.
7. Enter MAPI logon and RISS location information in the following boxes:
 - **Exchange Server:** Exchange server used when accessing the GAL for address resolution. XML tag is `<Server>`.
 - **Mailbox:** Mailbox on Exchange server used when accessing the GAL for address resolution. XML tag is `<Mailbox>`.
 - **SMTP Host:** DNS name or IP address of the RISS SMTP portal used to submit messages to RISS. XML tag is `<SMTPServer>`.
 - **Port:** SMTP port number. This setting is optional and the default is 25. XML tag is `<SMTPPort>`.
 - **HTTP Host:** Domain name or IP address of the RISS HTTP server queried when checking for duplicate messages. XML tag is `<HTTPServer>`.
 - **Domain:** RISS domain used when checking for duplicate messages to be submitted. RISS domain is case-sensitive and must match domain name in the `RISS Domain.jcml` configuration file. XML tag is `<RISSDomain>`.
 - **Repository:** Repository into which documents in the **Select Files To Process** list are delivered. XML tag is `<Repository>`.
 - **Audit Repository:** Name of repository that receives the PST Importer log file created during the import process. XML tag is `<AuditRepository>`.
8. To indicate mining and tombstone settings, select the following check boxes:

- **Use TNEF:** If selected, stores submitted messages in TNEF format. XML tag is `<UseTNEF>`.
- **Distribute To All Recipients:** If selected, PST Importer sends a copy of the document to all addresses specified in the message. If unselected, only the owner specified in the Repository box receives the document. XML tag is `<DistributeToAll>`.

If you do not select this setting, HP highly recommends using a repository that is not associated with an active email account. This prevents other mining processes, such as journal or mailbox mining, from introducing duplicate email messages into the specified repository.

- **Ensure Owner Receipt:** If selected, the specified repository receives a copy of the message whether or not the owner is specified in the To, From, Cc, or Bcc headers. This setting is especially useful for distribution lists and is selected by default. XML tag is `<EnsureOwnerReceipt>`.
 - **Force Processing:** If selected, messages in a PST file previously processed are tombstoned. Under normal circumstances, a PST file is not processed again unless it changes. This option forces Archive Request Loader and PST Importer to process the file again. XML tag is `<ForceProcessing>`.
 - **Create Tombstones in PST:** If selected, tombstoning for attachments is enabled. To tombstone the message body and attachments, also select the Trim Body from Tombstone check box. XML tag is `<Tombstone>`.
9. Click OK. The window shown in Figure 4-1 appears. The Select Input File to Process box contains the path and file name of the file created or revised. To validate the file from this point, continue to the next section.

Validating file using the Archive Request Loader user interface

1. Click Start > Programs > Hewlett-Packard > RISS PST Importer > Archive Request Loader, or enter `<install_path>/HPPSTInit` from the command line. The window shown in Figure 4-1 appears.
2. In the Select Input File to Process box, enter the path and file name of the Archive Request file to process, or click Browse to locate the file.
3. In the Provide Log File Location box, enter the path and file name of the Archive Request Loader log file, or click Browse to locate the file. The log

file contains processing and error information generated while loading the Archive Request file. If the log file already exists, the application appends processing and error information to the existing file.

Note: The log file's verbosity level is set to the default, which is 3 (information). To change the level, edit `RISS PST Importer.ini` and change the default `Verbosity` to the level of your choosing:

```
[HPPSTInit]
```

```
Verbosity=3
```

See [/v, on page 4-11](#) for an explanation of verbosity levels.

4. Click OK.

Validating file from command line

Use the `HPPSTInit` command with parameters to validate an Archive Request file:

```
<install_path>/HPPSTInit /i ArchiveRequestFileName.xml  
/o LoadLogFileName.log [/c] [/v5]
```

Parameter	Description
-----------	-------------

/i	Required. Name of input file to be processed. Replace <i>ArchiveRequestFileName.xml</i> with the full UNC path and XML file name.
----	--

Parameter	Description
/o	Required. Name of Archive Request Loader log file to which diagnostic and processing information is written. Replace <i>LoadLogFileName.log</i> with the full UNC path and log file name.
/c	Optional. Parses XML structure in input file for syntax and file accessibility only. No records are added to <i>PST.MDB</i> for processing.
/v	Optional. Verbosity level used when processing Archive Request file. Enter a number from 0 to 5 following the /v to indicate verbosity level, 5 containing the most detail. 0: Fatal 1: Alert 2: Warning 3: Information 4: Trace 5: Debug

PST Import Monitor

Use PST Import Monitor to:

- Start and stop import process.
- Display overview of running tasks, message counts, and other status information showing import progress.
- Draw attention to potential error conditions.
- Generate reports.
- Reset failed processes.

Using PST Import Monitor

1. To run PST Import Monitor, choose one of the following methods:
 - Click Start > Programs > Hewlett-Packard > RISS PST Importer > Import Monitor.
 - From the command line, enter the following command:
<install_path>/HPPSTStats.

The following window appears:

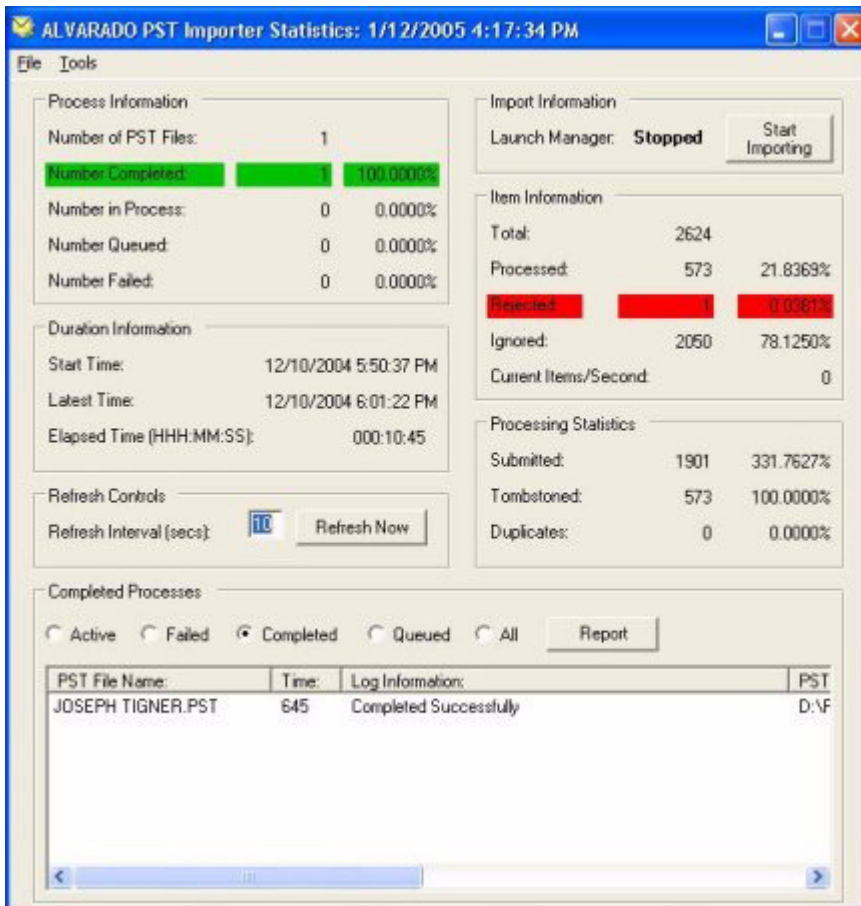


Figure 4-3: PST Import Monitor

2. PST Import Monitor displays basic data about the PST process status. To view specific processing information, see the following:

Item Information area:

- Total: Total number of items found in the PST files so far.
- Processed: Number and percentage of items processed and submitted to RISS.

- **Rejected:** Number and percentage of items that PST Importer could not process due to errors. The PST Importer log file contains error information explaining why the item was rejected. See [PST Importer log file, on page 4-15](#) for more information.
- **Ignored:** Number and percentage of items that were not processed because they cannot be submitted to RISS. These items include, but are not limited to, calendar items, tasks, contacts, and messages stubs.

Processing Statistics area:

- **Submitted:** Number and percentage of items processed and submitted to RISS.
- **Tombstoned:** Number and percentage of items submitted to RISS and replaced by tombstones in the PST files. This number is not cumulative and resets per run.
- **Duplicates:** Number and percentage of items not submitted to RISS because duplicate items already exist in imported PST files or duplicate items are already archived to RISS.

3. Complete any of the following tasks:

- To start the import process, click **Start Importing**.
- To stop the import process, click **Stop Importing**.
- To collect statistics immediately, click **Refresh Now**. Collecting statistics impacts performance.

PST Import Monitor automatically collects statistics according to the Refresh Interval specified. The default is 10 seconds. You can change the automatic refresh interval to any whole number between 1 and 60 seconds.

- To reset a failed process, select **Failed** under **Active Processes** to display a list of all failed processes, right-click the failed process, and click **Reset** (see Figure 4-4).

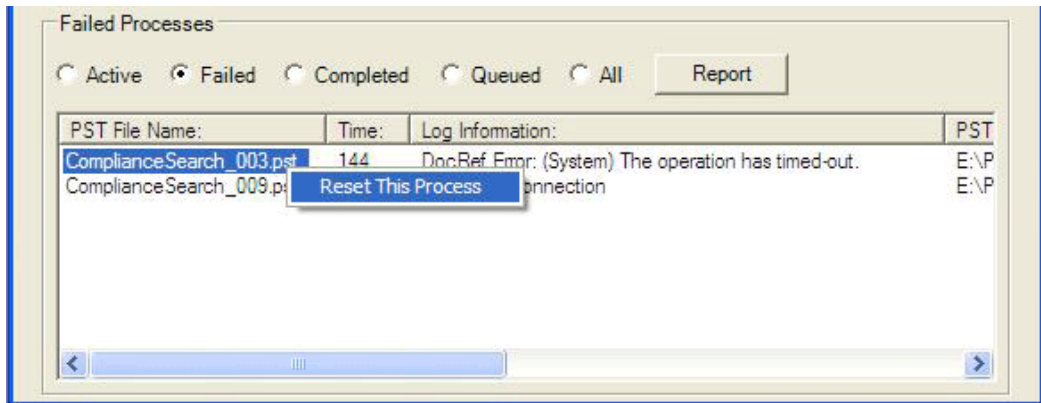


Figure 4-4: Resetting process

Depending on the reasons the process failed, resetting a failed process may not correct the problem. However, PST Importer tries to reprocess it as directed.

Displaying reports and log files

This section provides information about these reports:

- [PST Import report, on page 4-14](#)
- [Status Monitor report, on page 4-15](#)
- [PST Importer log file, on page 4-15](#)

PST Import report

Use PST Import Monitor to generate a PST Import report in HTML format. You can then import the report into a spreadsheet for analysis or progress tracking if needed.

1. Under Active Processes, select a process option, and click Report. A dialog box appears.
2. Specify where to save the report, and enter a file name. The default directory is `<install_path>\Reports`.
3. Click Save.

Status Monitor report

At each refresh interval, status information is automatically saved to `<install_path>/LogFiles/PSTImporterStats.log`. This is useful if the installation has its own separate process that monitors import progress. Modify the following RISS PST Importer.ini settings to specify a different path and file name for the report:

```
[PSTImporter]

MonitorPath=UNCPath
```

When the `MonitorPath` is specified, PST Importer creates the file specified by `UNCPath`. This file contains statistics displayed in PST Import Monitor. An external process can monitor and parse this file to determine the import status.

PST Importer log file

Each mining process is assigned a unique PST file and creates a PST Importer log file containing warnings, errors, and completion statistics about the process.

The log file is delivered to the repository specified by `<AuditRepository>` in the Archive Request file. The log file is sent as an email attachment. Upon successful submittal, the file is deleted.

If a mining process terminates and is retried, a separate log file is generated. Use the Web UI to determine the processing history of a PST file.

To change verbosity level, modify the following RISS PST Importer.ini settings, where `X` represents the verbosity level:

```
[PSTImporter]

Verbosity=X
```

The default verbosity level is 3 (information). See [/v](#), on page 4-11 for an explanation of verbosity levels.

Archive Request file

This section describes settings specified in an Archive Request file and provides a sample file.

Settings description

All settings specified under <Header> can be overridden at the <FileSpec> level. All settings described in the Archive Request file are required in either the <Header> or <FileSpec> sections unless otherwise noted.

Table 4-1: Tags in <Header>

Tag	Description
<Version>	Version number associated with this Archive Request format. Current version is 1.0.
<Server>	Exchange server used when accessing the GAL for address resolution.
<Mailbox>	Mailbox on Exchange server used when accessing the GAL for address resolution.
<SMTPServer>	DNS name or IP address of the RISS SMTP portal used to submit messages to RISS.
<SMTPPort>	Port number used with <SMTPServer>. This setting is optional. The default is 25.
<HTTPServer>	Domain name or IP address of the RISS HTTP server queried when checking for duplicate messages.
<RISSDomain>	RISS domain used when checking for duplicate messages to be submitted. RISS domain is case-sensitive and must match domain name in the RISS Domain.jcml configuration file.
<Repository>	Repository into which documents listed under <FileSpec> are delivered.
<AuditRepository>	Name of repository that receives processing logs created during the PST import process.

Table 4-1: Tags in <Header> (continued)

Tag	Description
<UseTNEF>	<p>Specifies if submitted messages are stored in TNEF format.</p> <p>True indicates TNEF format is used.</p> <p>False indicates TNEF format is not used.</p>
<DistributeToAll>	<p>Specifies if PST Importer sends a copy of the document to all addresses specified in the message.</p> <p>True enables this setting.</p> <p>False indicates only the owner specified in <Repository> receives the document. If set to False, HP highly recommends using a repository that is not associated with an active email account. This prevents other mining processes, such as journal or mailbox mining, from introducing duplicate email messages into the specified repository.</p>
<EnsureOwnerReceipt>	<p>Specifies if specified repository receives a copy of the message whether or not owner is specified in the To, From, Cc, or Bcc headers. This setting is especially useful for distribution lists. True enables this setting. False disables this setting.</p>
<ForceProcessing>	<p>Specifies if messages in a PST file that has been previously processed are tombstoned. Under normal circumstances, a PST file is not processed again unless it changes. This option forces Archive Request Loader and PST Importer to process the file again.</p> <p>The <ForceProcessing> tag is supported in the <Header> only. It cannot be applied to an individual <FileSpec> and is ignored if specified there.</p>
<Tombstone>	<p>Controls tombstoning:</p> <p>0: Tombstoning is not enabled.</p> <p>1: Only attachments are tombstoned.</p> <p>2: Both attachments and the message body are tombstoned.</p>
<FileSpecCount>	<p>Optional. Number of <FileSpec> tags listed later in the file. If provided, this tag controls file integrity by comparing the specified number to the actual number of <FileSpec> tags found.</p>

The <FileSpecList> contains a list of file specifications bounded by the <FileSpec> tag. The settings described for <FileSpec> are required unless otherwise noted.

Table 4-2: Tags in <FileSpec>

Tag	Description
<FilePath>	Path and file name of imported file. Wildcards are allowed and are expanded prior to processing. UNC paths are supported and highly recommended.
<ProcessingType>	Type of import processing to be performed on the <FilePath>. PST is the only processing type supported in current release.
<DistributeToAll> <Server> <Mailbox> <SMTPServer> <SMTPPort> <HTTPServer> <RISSDomain> <Tombstone> <UseTNEF> <Repository> <AuditRepository> <EnsureOwnerReceipt>	Optional. Use them at the <FileSpec> level only to override <Header> settings.

Sample file

```
<?xml version="1.0" encoding="UTF-8"?>
<ArchiveRequest>
  <Header>
    <Version>1.0</Version>
    <Server>pleexc01</Server>
    <Mailbox>dmontgomery</Mailbox>
    <SMTPServer>papoon</SMTPServer>
    <SMTPPort>25</SMTPPort>
    <HTTPServer>papoon</HTTPServer>
    <RISSDomain>firesign</RISSDomain>
    <Repository>user@firesign.dev</Repository>
    <AuditRepository>audit@firesign.dev</AuditRepository>
    <UseTNEF>True</UseTNEF>
    <DistributeToAll>True</DistributeToAll>
    <EnsureOwnerReceipt>True</EnsureOwnerReceipt>
    <ForceProcessing>True</ForceProcessing>
    <Tombstone>1</Tombstone>
    <FileSpecCount>3</FileSpecCount>
  </Header>
  <FileSpecList>
    <FileSpec>
      <FilePath>
        E:\PSTFiles\Persist Search Results.pst
      </FilePath>
      <ProcessingType>PST</ProcessingType>
    </FileSpec>
    <FileSpec>
      <FilePath>
        E:\PSTFiles\ComplianceSearch_001.pst
      </FilePath>
      <ProcessingType>PST</ProcessingType>
    </FileSpec>
    <FileSpec>
```

```
<FilePath>
  E:\PSTFiles\Outlook.pst
</FilePath>
  <ProcessingType>PST</ProcessingType>
</FileSpec>
</FileSpecList>
</ArchiveRequest>
```

CHAPTER 5

Configuring Outlook or Lotus Notes

This chapter contains information about these topics:

- [Configuring your system for Exchange and Outlook, on page 5-2](#)
- [Configuring your system for Domino and Lotus Notes, on page 5-14](#)

Configuring your system for Exchange and Outlook

This section contains information about these topics:

- [Configuring user accounts on customer servers, on page 5-2](#)
- [Configuring Journal Mining, on page 5-3](#)
- [Configuring Mailbox Mining, on page 5-5](#)
- [Installing the Outlook plug-in, on page 5-8](#)

Configuring user accounts on customer servers

Table 5-1 illustrates how to configure user accounts for Selective Archiving.

Table 5-1: User accounts on customer servers

For	User type and mailbox location	Default last name, user logon (password), alias ^a	Group membership or permissions
Mailbox Mining	Domain user and mailbox on Exchange servers	Appuser, appuser (skyline); alias=appuser	Administrators, Exchange Domain Servers

Table 5-1: User accounts on customer servers (continued)

For	User type and mailbox location	Default last name, user logon (password), alias^a	Group membership or permissions
Journal Mining	Active Directory user and mailbox on Exchange servers	LocalJournalUser, LocalJournalUser (skyline); alias=LocalJournalUser	User
Dynamic Account Synchronization	Active Directory user on servers where user accounts exist	appuser, appuser (skyline) [or an existing user]	Read access to user objects and the following properties: <ul style="list-style-type: none">• objectGUID• givenName• mail• sn• whenChanged• whenCreated• distinguishedName• proxyAddresses• uSNChanged• userAccountsControl• manager• directReports• sAMAccountName

^a. The same user account can be used for more than one of these activities.

Note: All Email Miners must join the domain. Email Miners are named EM-SO-110-1, EM-SO-110-2, and so on.

Configuring Journal Mining

Journal mining is the standard process for draining email from Microsoft Exchange servers.

Table 5-2: User accounts for Journal Mining

For	User type and mailbox location	Default last name, user logon (password), alias ^a	Group membership or permissions
Selective archiving	Domain user and mailbox on Exchange servers	Appuser, appuser (skyline); alias=appuser	Administrators, Exchange Domain Servers

^a. The same user account can be used for more than one of these activities.

Setting registry key for journaling

To implement envelope or BCC journaling, set the registry key. Envelope journaling captures all recipient information including BCC and distribution lists. BCC journaling saves BCC recipient information.

On each Exchange server to be mined, set the registry key to journal messages and save envelope or BCC information. The customer's Exchange administrator must perform this task or give you the necessary credentials. For more information, see the following web site.

<http://support.microsoft.com/default.aspx?scid=kb;en-us;843105&Product=exch2k>

Enabling journaling on mailbox stores

To enable journaling on selected mailbox stores, you or the local Exchange administrator must set mailbox store properties using Exchange System Manager. This procedure requires the local journal user and mailbox that were created earlier (see [Table 5-1, on page 5-2](#)). LocalJournalUser is the default.

1. Log on to an Exchange server.
2. To start Exchange System Manager, select Start > Programs > Microsoft Exchange > System Manager.
3. Open the Servers folder.
4. For each server listed:
 - a. Click the Server tab.

- b. Open a Storage Group.
 - c. Right-click Mailbox Store, and select Properties.
 - d. Click General.
 - e. Select Archive all messages sent or received by mailboxes in this store.
 - f. Click Browse.
 - g. Select journal user and mailbox where messages from the mailbox store are copied.
 - h. Click OK twice.
 - i. Repeat step b through step h for each Storage Group on the server.
10. Repeat this procedure on other Exchange servers as needed to set up other mailbox stores for journaling.

Configuring Mailbox Mining

Mailbox mining, also known as selective archiving, uses rules to archive email from a Microsoft Exchange server to RISS. The system is first queried to determine if the email in a user's mailbox is already archived. If it is, a stub is created in the Exchange server. A stub is a link to the original email that is stored in the system. If the email is not already archived, it is archived, and a stub is created.

Mailbox mining must be configured on Exchange servers and Outlook clients.

Configuring Exchange for email stub support

Before publishing the Outlook template, generate a forms registry so the Outlook form can be published to the system. This procedure requires you or the Exchange administrator to log on the Exchange server with administrator permissions.

1. Log on the Exchange server as Administrator.
2. To start Exchange System Manager, select Start > Programs > Microsoft Exchange > System Manager.
3. In the left-hand pane, expand Folders.
4. Right-click Public Folders, and select View System Folders.
5. In the left-hand pane, expand Folders.
6. Right-click EFORMS REGISTRY, select New, and click Organizational Form.
7. Name the form Platform, and click OK.
8. In the left-hand pane, expand EFORMS REGISTRY.
9. Right-click Platform, and select Properties.
10. In the Properties dialog box, click Permissions, and click Client Permissions.
11. In the Client Permissions dialog box, click Add.
12. In the Add User dialog box, double-click the domain user created for selective archiving, and click OK.
13. From the Role drop-down list in the Permissions section, select Owner, and click OK.
14. Click OK. The Properties dialog box closes.

Publishing forms

After the forms registry has been created, publish the form using Outlook. Perform the following steps on any computer with an Outlook client that can connect to the Exchange server.

1. Create an Outlook Profile accessing the Exchange server with the domain user (appuser).

2. Run Outlook using the profile created.
3. In Outlook, select Tools > Forms > Design a Form.
4. From the Look In list in the Design Form dialog box, select User Templates in File System.
5. Click Browse, and select the drive containing the RISS Utilities CD, select the Exchange folder, and select the PERSISTMailItem form (PERSISTMailItem.oft). Click OK. The PERSISTMailItem form appears in the Design Form dialog box.
6. Select the PERSISTMailItem form, and click Open.
7. In the Form Editor window, select Tools > Forms > Publish Form as.
8. From the Look In drop-down list, select Organizational Forms Library.
9. In the Display name and Form name boxes, enter PERSISTMailItem, and click Publish.
10. After publishing the form, close the form editor without saving the form, and close Outlook.

Configuring non-sticky ports

A non-sticky port (port 81) is provided to allow load balancing of hash lookups on a message-by-message basis for client applications.

To make an email miner use the non-sticky port:

1. Start the EMS Scheduler application.
2. Find a Sherpa CSV (Mailbox Mining) event.
3. Find the DocRef Host setting. This should contain the IP address/Host name of a VIP.
4. Add the port number by appending a colon followed by the port number to the IP address/Host name For example,

DocRef Host: HTTPHOST: 81

5. Click Apply.

6. Close the EMS Scheduler application.
7. Restart the Launch Manager service to make the new setting take effect.

Repeat this procedure as needed for all Mailbox Mining events.

Installing the Outlook plug-in

The HP RISS Outlook plug-in is a “COM Add-In” for Microsoft’s Outlook application. After the plug-in is installed and configured, it provides the end-user with seamless integration to RISS and facilitates retrieval of tombstoned messages and search results.

A user with local administration privileges must install the plug-in. The installation adds registry entries in the `HKEY_LOCAL_MACHINE` key and, therefore, the user installing the software must have sufficient privileges. After the plug-in is installed, all users on the machine can access the plug-in when they start Outlook.

Running the “MSI” copies and registers the necessary components in the `C:\Program Files\Persist\HP RISS Outlook Plugin` folder. Upon installation, initial registry settings are made in `HKEY_LOCAL_MACHINE` (HKLM). The first time a user runs Outlook on a machine that has the plug-in installed, these registry settings are copied from HKLM to `HKEY_CURRENT_USER` (HKCU). These registry settings are then maintained on a user-by-user basis in HKCU by selecting Tools: Options: Archive Options from Outlook’s main menu.

Registry settings

To change default settings for all users, use `REGEDIT` to make changes in HKLM so they are copied and saved to HKCU when each user first runs Outlook. The following defaults are set in the registry:

- Cache-related registry settings
 - `[HKLM\Software\Persist\Outlook PlugIn\Cache]`

`UseCache=True`: Indicates if the plug-in caches messages retrieved from RISS. The default is `True`. Changing this to `False` causes the Location specified below to be automatically emptied when Outlook is closed. This is a user-configurable setting.

CacheEML=True: The default is True, which indicates the intermediate .eml file is cached for the message being retrieved from RISS. Setting this to False causes the .eml file to be deleted when it is no longer needed. This setting is ignored if UseCache=False. This is a user-configurable setting.

CacheMsg=True: The default is True, which indicates the resultant .msg file is cached for the message being retrieved from RISS. Setting this to False causes the .msg to be deleted when it is no longer needed. This setting is ignored if UseCache=False. This is a user-configurable setting.

Location=: Folder in which cache is located. The administrator should not assign a value to this registry value in HKLM. It is initialized in HKCU to \Documents and Settings\CurrentUser\Local Settings\Application Data\Persist\Cache upon the first execution for a user. This is a user-configurable setting.

MaxSize=20: Size, in megabytes, of cache folder. When this size is exceeded, .eml and .msg files are deleted according to a Least Recently Used algorithm until the size of the cache again below the limit specified by this setting. This is a user-configurable setting.

- RISS retrieval-related registry entries

These settings are used for Offline Cache Management, Message Export, and retrieval of messages within the Outlook User Interface itself.

- [HKLM\Software\Persist\Outlook PlugIn\PlugInURLs]

FetchURL0=http://HOSTNAME/externalAPI/servlet/DocumentRetrievalServlet?documentURL=#REF#: URL the plug-in uses to retrieve tombstoned messages. The HOSTNAME must be changed to indicate the name or IP address of RISS.

FetchURLX=: The X in this setting represents a number in the range of 1 to 9. If the plug-in fails to retrieve a tombstoned message using FetchURL0, it attempts to retrieve the message using FetchURL1 through FetchURL9 sequentially.

- Search and export related registry entries

- [HKLM\Software\Persist\Outlook PlugIn\Search]

AllowExternalFolderSupport=True: When True, the user is restricted from saving PST files to an external location. This is an

administrator/diagnostic setting and should be modified only at the direction of Support Personnel.

DefaultFolder=Default: Name of folder within generated PST files into which the Message Export Facility downloads archived messages. This is a user-configurable setting.

PSTFileFolder=C:\PSTFiles: File system folder used to store individual PST Files when **UseExternalFolderSupport=True**. This is a user-configurable setting.

PSTFilePrefix=ComplianceSearch: File name prefix used to create individual PST Files when **UseExternalFolderSupport=True**. Each file begins with the specified prefix specified and has an ordinal appended to the filename. (for example, **ComplianceSearch_001.pst** or **ComplianceSearch_002.pst**) This is a user-configurable setting.

RetrievalHost=HOSTNAME: This setting has been deprecated and is no longer used.

RetrievalURL=http://#HOST#/externalAPI/servlet/DocumentRetrievalServlet.asp?documentURL=#REF#: URL used to retrieve results of a search specified in the RISS Web User Interface. This setting should be modified only at the direction of Support Personnel.

SearchURL=http://HOSTNAME: URL the plug-in uses to launch the Web User Interface for search purposes. Change **HOSTNAME** to indicate the DNS name or IP address of RISS. This is a user-configurable setting.

UseExternalFolderSupport=True: Specifies if the Message Export Facility allows the user to save PST files to an external location. The default is **True**. When **UseExternalFolderSupport=True**, the Message Export Facility saves generate PST files prefixed with **PSTFilePrefix** to the folder specified by **PSTFileFolder**. This is a user-configurable setting.

- Administrative registry settings

- [HKLM\Software\Persist\Outlook PlugIn]

- AdminMode=False:** Indicates this machine is in Administrative mode. The default is **False**. When set to **True**, the user is restricted from changing user-configurable settings.

LogFilepath=: Fully-qualified path name where the plug-in records diagnostic information. This is an administrator/diagnostic setting and should be modified only at the direction of Support Personnel.

Manually creating other registry settings

To repackage the installation for deployment with Software Management Server (SMS) or other client management tool, components must be registered.

In the settings described below, @ indicates the default for the key specified. Some settings only create the key, and specific values are not created.

In addition to registering components, a file association must be created to properly launch the Message Download Facility. To create this file association, create the following registry entries:

- [HKLM\SOFTWARE\Classes\dldFile]
 - @=Message Export Control File: Text displayed in Windows Explorer when a file with a .dld extension is encountered.
- [HKLM\SOFTWARE\Classes\dldFile\shell\Open]
 - @=&Open with PTBatch: Description that appears in the context menu under the Open With setting when a user right-clicks on a .dld file.
- [HKLM\SOFTWARE\Classes\dldFile\shell\Open\command]
 - @="[INSTALLDIR]PTBatch.exe" "%1": Executable launched when a user clicks Open as Internet Explorer asks whether the user wishes to open or save the .dld file. Double-clicking on a .dld file in Windows Explorer also uses this setting to launch the Message Export Facility.
- [HKLM\SOFTWARE\Classes\.dld]
 - @=dldFile: Key that associates the .dld extension with the registry settings described above.
- [HKLM\SOFTWARE\Classes\.dld\dldFile]
 - Create the registry key only.
- [HKLM\SOFTWARE\Classes\.dld\dldFile\ShellNew]
 - Create the registry key only.

To properly install the plug-in for users other than the administrator who installs it, make the following settings in HKLM:

- [HKLM\Software\Microsoft\Office\Outlook\Addins\PTOutlookArchive.Connect]
 - FriendlyName=Hewlett-Packard Outlook Add-in
 - Description=Hewlett-Packard Outlook Add-in
 - LoadBehavior=dword:00000003
 - CommandLineSafe=dword:00000000

Installing and configuring the Outlook plug-in for users

1. On the user's computer, close Outlook if open, and install the HP RISS Outlook plug-in by running `setup.exe` on the Utilities CD.
2. Follow the Install Shield wizard instructions.
3. Open Outlook. The Search Archive button is displayed in Outlook.
4. Select Tools > Options. The Options dialog box appears.
5. Click Archive Options. The Archive Options panel appears.
6. In the URL to Modify (Fetch URL) list, select the default URL to display it in the URL to Modify box, and edit the URL. Replace HOST with the DNS name associated with the virtual IP (VIP) web user interface for the system.
7. In the Search URL box, enter the internet address of RISS. Replace HOST with the DNS name associated with the VIP web user interface for the system.
8. Click OK.
9. In Outlook, click Search Archive. A browser window with the logon page for the Web Interface appears. If it does not, the DNS names specified previously in the Archive Options panel are incorrect.

Note: For more information about the Archive Options panel of the Options dialog box, see the “System administrator tasks” section of the user guide.

Configuring your system for Domino and Lotus Notes

This section contains information about configuring your system to enable Lotus Notes selective archiving. This section covers these topics:

- [*Requirements for Domino server configuration, on page 5-14*](#)
- [*Installing Email Miner for Lotus Notes, on page 5-15*](#)
- [*Administering Email Miner for Lotus Notes, on page 5-15*](#)
- [*Installing and configuring the Lotus Notes plug-in, on page 5-15*](#)

Requirements for Domino server configuration

To configure your Domino server to enable Lotus Notes selective archiving, you might need to perform the following tasks:

1. Configure the LDAP service. Because LDAP is not mandatory on Domino servers, you might need to enable this service.

For the most up-to-date instructions on setting up a Domino LDAP Service, starting and stopping the LDAP Service, and setting up users, see the Lotus Notes LDAP client documentation and the Lotus Notes R5 Help.

After you enable LDAP for the Domino server, clients and LDAP-enabled applications can query the Domino server and get information about entries in the Domino Directory.

2. Configure journaling. You must configure all Domino servers that interact with the RISS system for journaling by the Domino administrator. See the Lotus Notes documentation for more information.
3. Configure Lotus DIRCAT. Your Lotus Notes environment might include Lotus DIRCAT. If your system does include Lotus DIRCAT, see the Notes Domino R5/6.x documentation for information about implementing this service.

Installing Email Miner for Lotus Notes

The Email Miner for Lotus Notes is an application (`miner.nsf`) loaded to and signed by the Domino Servers. Your HP installer performed the initial installation on the HP Gateway server. See [Email Miner Version P2.0 for Lotus Notes Installation Guide, on page A-1](#), for more information.

Administering Email Miner for Lotus Notes

See [Email Miner Version P2.0 for Lotus Notes Administration Guide, on page B-1](#), for information about administering email miner.

Installing and configuring the Lotus Notes plug-in

The HP installer works with the system administrator to update `<install dir>\lotus\notes\Notes.ini` on the Notes Client to reference the Notes plug-in by adding the following lines at the end of the file:

```
EXTMGR_ADDINS=nhpclient.dll  
  
RISS_DOMAIN_NAME=(RISS domain name, for example, csf.store  
  
RISS_HOST_ADDRESS= (IP address of the RISS system
```

where domain name and host name define the RISS system used to archive the emails.

The system administrator is responsible for installing the Notes Plug-in file `nHPClient.dll` on every Lotus Notes user's client. It is not installed on any server. On the client machine, it is placed in the `\lotus\notes` subdirectory.

APPENDIX A

Email Miner Version P2.0 for Lotus Notes Installation Guide

This appendix contains the following information.

- [Overview, on page A-2](#)
 - [Architecture, on page A-2](#)
 - [Frequently asked questions, on page A-2](#)
 - [System requirements and prerequisites, on page A-5](#)
 - [Available platforms and restrictions, on page A-6](#)
- [Email Miner, on page A-7](#)
 - [Installation, on page A-7](#)
- [Error messages, on page A-12](#)

Overview

Email Miner is a Lotus Notes mail administration product that mines documents from mail databases and/or journal databases and places the documents within the RISS architecture.

Architecture

The Email Miner databases must be installed on every mail server that requires processing. This is because all Email Miner activity is done locally, meaning that no network connectivity occurs while Email Miner is processing the databases. Each Email Miner server only processes the databases that have that server assigned as the home server within the Name and Address Book.

During the installation process, three Email Miner agents will be created for each server on which Email Miner is installed. This agent will process all Mail Restrictions that the administrators have created. Each Mail Restriction can be as detailed as you desire, meaning you can have a Mail Restriction span the entire enterprise or you can create one specific to a mail server and/or mail user. Each Mail Restriction must be assigned a priority, and this priority determines the Mail Restriction that applies to each mail user.

Frequently asked questions

Architecture

Question	Answer
What version of Domino must my servers be running?	Email Miner requires that your servers are running either 5.x or 6.x.
What files are placed on my Domino server?	Email Miner is self-contained within two Lotus Notes databases. There are no other files to be placed on the servers.
How does Email Miner work?	Email Miner uses a scheduled LotusScript agent to perform all of the processing.

Question	Answer
Does Email Miner update my Name and Address Book?	No. All Name and Address Book accesses are references (read) only.
Does Email Miner update my notes.ini?	No. There are no .ini settings required.
How does Email Miner work with clustered servers?	Clustering does not affect Email Miner. The home server's agent processes each mail database, unless specific configuration is done within Email Miner to have processing occur on the clustered server.
Does Email Miner work on partitioned servers?	Yes. Partitioning has no affect on Email Miner.
Does Email Miner work with shared mail?	Yes. Shared mail has no effect on Email Miner.
What mail templates are compliant with Email Miner?	Any mail template that was supplied by Lotus is functional with Email Miner.
Are customized mail templates a problem?	No. Email Miner will simply process whatever folders/views are specified, whether they are generic or specific.
How many versions of Email Miner do I need if my servers have different platforms?	One. There are no platform-specific versions of Email Miner.

Permissions

Question	Answer
What access does Email Miner require to the mail databases?	Email Miner only requires 'Editor' access.
Whose permissions is Email Miner using to access the mail databases?	Whatever ID (Server/user) signed the Email Miner agent, is the ID being used to process the mail databases.
Can I sign the Email Miner agent with my server ID?	Yes. This is a very common practice. Some companies also choose to use a 'generic' administration ID to sign the agents.

Migration

Question	Answer
What must I do when I migrate my servers from R5 to R6?	Nothing. The same version of Email Miner can process on an R5 or an R6 server.
What must I do when I migrate my servers' operating systems?	Nothing. There is only one code-stream for Email Miner.

Installation

Question	Answer
How do I install Email Miner?	An installation database is provided that will perform all of the installation steps.
Do I need to physically visit every server?	No. All server installations can be performed from your Lotus Notes client.
Do I need to bring my server down/up after installing Email Miner?	No. This is not required or needed.
How do I uninstall Email Miner?	Simply delete the Email Miner databases and the product is uninstalled.

Upgrade

Question	Answer
How do I upgrade Email Miner?	Within the installation database there is an upgrade procedure that will guide you through the upgrade steps.

Question	Answer
Must I upgrade every server (replica) of Email Miner?	No. The upgrade only needs to be performed on one server, providing that the Email Miner database can properly replicate to all other replicas.
What happens to the Email Miner data when I upgrade?	Nothing. All of the data remains intact.
Will I need to re-sign the agents after upgrading?	No. When the Email Miner agents were originally created, they were protected so that design refresh/replace would not affect them.

Configuration

Question	Answer
Can I centrally administer Email Miner?	Yes, providing that Email Miner is properly replicating to all servers that contain a replica.
Can I selectively restrict the Email Miner data?	Yes. Email Miner can be configured to reflect your replication topography, thus only allowing each mail server to contain its own information.

System requirements and prerequisites

System requirements

- 256 MB RAM per server
- 200 MB free disk space per server
- Each server must be running Lotus Notes 5.x or 6.x

Prerequisites

- Email Miner agent signer must have 'Run Restricted LotusScript Agents' rights and 'Administrator' rights

- Set 'Max LotusScript execution time' to at least 120 minutes. The Email Miner agent could be very extensive depending upon many factors, such as number of mail users
- Email Miner installer must have 'Create new databases' and 'Create replica databases' rights
- AMGR must be running as a server task
- Router must be running to allow proper error notification
- Replica must be running to allow proper replication

Available platforms and restrictions

Email Miner has been successfully tested/implemented on the AS/400, S/390, AIX, Linux, OS/2, Sun/Solaris, HP/UX, Netware and Windows platforms. The Email Miner design is completely platform independent.

There are no platform specific restrictions.

Email Miner

Installation

The installation database **MUST** be located on a Lotus Notes server and can reside in any directory within the Notes data structure.

Note: If Email Miner already exists on the installation server, the installation database **MUST** be located within the directory where Email Miner resides.

The Email Miner installation will create the Email Miner databases, Server Definitions, agents, and propagate /replicate the Email Miner databases to all specified servers (if more than one server was specified and 'Automatically create replicas' was selected).

Initial installation

If you have not installed Email Miner on any server within your infrastructure, you will need to perform an 'Initial Installation'. If you have already installed Email Miner on at least one server, and you want to now place it on additional servers see 'Additional Servers Installation'.

For an Email Miner 'Initial Installation', perform the following steps:

1. Select Actions | 1. Initial Installation

INSTALLATION	
Installation	
Servers	Server1/ACME Server2/ACME
Managers	John Smith/ACME LocalDomainServers
Options	<input checked="" type="checkbox"/> Automatically create replicas <input checked="" type="checkbox"/> Delete existing databases

To start the installation, click [Install](#)

Bold field text denotes required field

Figure A-1: Initial installation

2. Specify the values

- Use Servers to specify the servers where Email Miner is to be installed.

Note: This field will be automatically populated with the name of the server where the Installation database resides.

- Use Managers to specify the entries that are to be placed into the ACL as 'Manager' within the Email Miner databases.

Note: This field will be automatically populated with the name of the person performing the installation and 'LocalDomainServers'.

- Use Options to specify the installation options.

Select Automatically create replicas if you want to create the Email Miner replicas during the Installation. If you do NOT select this option, the Email Miner replicas will not be automatically created and must then be deployed manually.

Select Delete existing databases if you want the installation process to delete any existing Email Miner databases that might exist on the selected servers. If you do NOT select this option, the installation will skip any servers that currently contain the Email Miner databases.

3. Install

- Click Install to begin the installation.

The installation process will display the tasks being performed. The results from this process are saved within the installation database.

Additional servers installation

If Email Miner already exists on at least one server in your infrastructure AND you want to install it on additional servers, you will need to perform an 'Additional Servers Installation'. If you have NOT installed Email Miner on any server within your infrastructure, see 'Initial Installation'.

For a Email Miner 'Additional Servers Installation', perform the following steps:

1. Select Actions | 2. Additional Servers Installation

Install'."/>

Installation

Servers

Server3/ACME
Server4/ACME

Options

☒ Automatically create replicas
☒ Configure server definition
☒ Delete existing databases

Method

☒ Combine ☐ Model

Server definition

To start the installation, click [Install](#)

Bold field text denotes required field

Figure A-2: Additional Servers installation

2. Specify the values

- Use Servers to specify the servers where Email Miner is to be installed.
- Use Options to specify the installation options.

Select Automatically create replicas if you want to create the Email Miner replicas during the installation. If you do NOT select this option, the Email Miner replicas will not be automatically created and must then be deployed manually.

Select Configure server definition if you want the Server Definitions that will be created by the installation to either combine with an existing Server Definition or to be modeled after an existing Server Definition.

Select the Method that you wish to use for the Server Definitions.

Select the Server definition that is to be used. The dropdown will display the current Server Definition documents found within the existing Email Miner database.

Select Delete existing databases if you want the installation process to delete any existing Email Miner databases that might exist on the selected servers. If you do NOT select this option, the installation will skip any servers that currently contain any Email Miner database.

3. Install

- Click Install to begin the installation.

The installation process will display the tasks being performed. The results from this process are saved within the installation database.

Upgrade

The installation database **MUST** be located on a Lotus Notes server and **MUST** be placed within the directory where Email Miner currently resides.

The upgrade will replace the existing design of Email Miner. This new design will be integrated via templates of the Email Miner databases that are attached within a document in the installation database. You will be prompted to select the template that should be used for the design replacement for the specified databases. Follow the upgrade directions carefully, so that the proper template is selected for the appropriate Email Miner database.

Note: Since other processes are also performed during the upgrade, do not attempt to upgrade Email Miner in any other manner.

Note: The Email Miner agents that were created during the installation process are not updated during the upgrade process, which will preserve the agent signers.

For a Email Miner 'Upgrade', perform the following steps:

1. Select Actions | 1. Email Miner | 3. Upgrade



UPGRADE

To start the upgrade, click [Upgrade](#)

Bold field text denotes required field

Figure A-3: Upgrade

2. Upgrade

- Click Upgrade to begin the upgrade.

The upgrade process will display the tasks being performed. The results from this process are saved within the installation database.

Note: When the 'Replace Design' dialog box appears, be sure to select the 'Email Miner' (miner.ntf) template for the 'miner.nsf' database, and the 'Email Miner Reference' (referenc.ntf) template for the 'referenc.nsf' database.

Error messages

The Installation database can generate numerous error messages. Each error message is categorized as either 'expected' or 'unexpected'.

An 'expected' error is caused by a configuration problem within the installation database. Email Miner generates all 'expected' errors and each error will begin with 'ERRxxxx' (where 'xxxx' is the specific error number).

An 'unexpected' error is caused when the installation database encounters an error from LotusScript that was not expected. These errors are passed directly on to the installation log.

If an error is reported by the installation database and is NOT in any of the lists, please contact HP technical support.

Table A-1: Installation Error Messages

Error number	Error message	Cause	Action
ERR0001	Could not find Server Definition for 'xxx'	The Server Definition for the specified server ('xxx') cannot be found within Email Miner.	Contact HP technical support.
ERR0002	You must place the installation database on a domino server	The installation database does not currently reside on a server (KitType = 2).	Move the installation database to a Domino server.
ERR0003	Could not find the 'Email Miner' templates	The templates for the Email Miner databases cannot be found within the installation database.	Contact HP technical support

Table A-1: Installation Error Messages (continued)

Error number	Error message	Cause	Action
ERR0004	Unable to delete 'xxx\miner.nsf'	The Email Miner database 'xxx\miner.nsf' (where 'xxx' is the directory structure) is either locked by another process or you do not have sufficient access to delete the database.	Adjust the ACL of the Email Miner database and/or delete the database using another method and retry the installation. If the problem persists, contact HP technical support.
ERR0005	Unable to delete 'xxx\referenc.nsf'	The Email Miner database 'xxx\referenc.nsf' (where 'xxx' is the directory structure) is either locked by another process or you do not have sufficient access to delete the database.	Adjust the ACL of the Email Miner Reference database and/or delete the database using another method and retry the installation. If the problem persists, contact HP technical support.
ERR0006	Could not find agent 'Email Miner'	The installation cannot find the agent ('Email Miner') needed to create the server-specific agents.	Contact HP technical support.
ERR0007	Could not find agent 'Email Miner RISS'	The installation cannot find the agent ('Email Miner RISS') needed to create the server-specific agents.	Contact HP technical support.

Table A-1: Installation Error Messages (continued)

Error number	Error message	Cause	Action
ERR0008	Could not find agent 'Email Miner Tombstone'	The installation cannot find the agent ('Email Miner Tombstone') needed to create the server-specific agents.	Contact HP technical support.
ERR0009	Insufficient access to 'xxx\miner.nsf' (yyy) on server 'zzz'	You only have 'yyy' (where 'yyy' is the access level) access to the Email Miner database (where 'xxx' is the directory structure) on 'zzz' (where 'zzz' is the server name).	Assign 'Manager' access to the User ID being used, within the ACL of the Email Miner database.
ERR0010	Insufficient access to 'xxx\referenc.nsf' (yyy) on server 'zzz'	You only have 'yyy' (where 'yyy' is the access level) access to the Email Miner Reference database (where 'xxx' is the directory structure) on 'zzz' (where 'zzz' is the server name).	Assign 'Manager' access to the User ID being used, within the ACL of the Email Miner Reference database.

APPENDIX B

Email Miner Version P2.0 for Lotus Notes Administration Guide

This appendix contains information about the following topics:

- [Email Miner, on page B-2](#)
 - [Overview, on page B-2](#)
 - [Security, on page B-2](#)
 - [Mail server configuration, on page B-3](#)
 - [Mail user configuration, on page B-9](#)
 - [Selective archiving, on page B-13](#)
 - [Agents, on page B-19](#)
- [Error messages, on page B-20](#)
 - [Dialog Box messages, on page B-20](#)
 - [Email notifications, on page B-21](#)
 - [Log messages, on page B-21](#)

Email Miner

Overview

Email Miner uses Mail Restrictions to locate the documents that are to be placed within the RISS architecture. Information for each document that matches the specified criteria is added to the Email Miner reference database. This information is then used to place the document within the RISS.

Security

Below is a table that describes how Email Miner is secured.

Security	Description
Access Control List	During the Installation process, the Email Miner ACL is set to reflect a typical environment.
Roles	Email Miner uses Roles for additional security. All of the 'Administration' forms and views are all Role-protected (using 'DB Manager'). Roles are also used to allow servers to replicate any document (using 'DB Reader').
Secured Forms	The 'DB Manager' Role protects all forms that are preceded with 'Administration'. If the User ID in use does not have the 'DB Manager' Role assigned, the 'Administration' forms will not be available to that user.
Secured Views	All views that are preceded with 'Administration' are all protected by the 'DB Manager' Role. If the User ID in use does not have the 'DB Manager' Role assigned, then the 'Administration' views will not be available to that user.
Document Protection	All documents use 'Authors' and 'Readers' to ensure document security.
View Protection	All of the Mail User views (non-Administration) are set to prohibit document insertion (paste).

Mail server configuration

There are two components for every mail server.

- Server Definition

The Server Definition defines the characteristics of each mail server. A Server Definition will automatically be created for each mail server during the Email Miner Installation. Each mail server must be included on a Server Definition and if one does not exist, Email Miner will email the administrators of the problem.

- Server Status

The Server Status is automatically created for each mail server, when the Email Miner agent executes and contains processing information for the mail server.

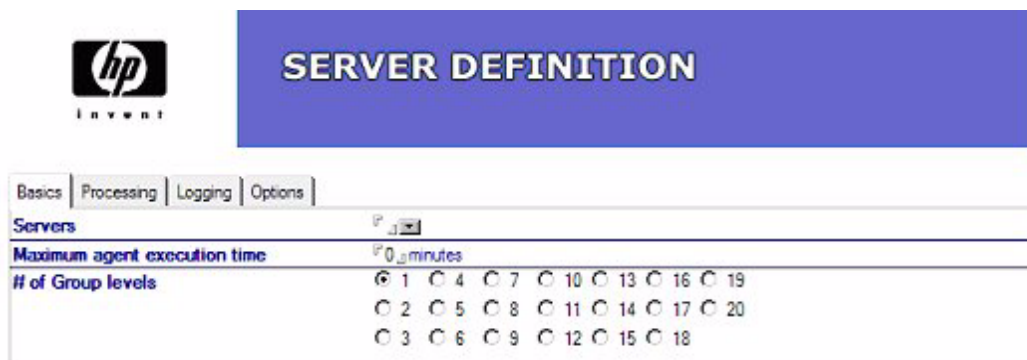
Server definition

A Server Definition is a Email Miner document that is required for every server on which Email Miner runs. It defines basic information required for every server.

Note: All servers selected during the Email Miner Installation should already have a Server Definition document.


To create and complete a new Server Definition, perform the following steps:

1. Select Create | Administration | 1. Server Definition



SERVER DEFINITION

Basics | Processing | Logging | Options

Servers 

Maximum agent execution time ☒ 0 minutes

of Group levels

☒ 1 ☐ 4 ☐ 7 ☐ 10 ☐ 13 ☐ 16 ☐ 19
☐ 2 ☐ 5 ☐ 8 ☐ 11 ☐ 14 ☐ 17 ☐ 20
☐ 3 ☐ 6 ☐ 9 ☐ 12 ☐ 15 ☐ 18

Bold field text denotes required field

Figure B-1: Server Definition

2. Specify the 'Basics' values

- Use Servers to specify the servers that should be included within the Server Definition. All servers within the same Server Definition will have the same characteristics/properties.
- Use Maximum agent execution time to specify how long the Email Miner agent can run. It is recommended that you set this time to be at least 10 minutes shorter than the time set in the 'Maximum Agent Execution Time' in the Directory (Name and Address Book). Doing this will allow Email Miner to shut down the agent properly.
- Use # of Group levels to specify how many levels of group membership is used within your groups in the Directory. Email Miner will only check the specified number of levels for all group membership processing.

3. Specify the 'Processing' options

Basics	Processing	Logging	Options
RISS email address		P...	
Maximum queue size		P0	
Options		<input checked="" type="checkbox"/> Journal <input checked="" type="checkbox"/> Selective	
Journal		Selective	
File paths		Pmailrn.nsf	
Options		<input checked="" type="checkbox"/> Delete after sending	

Figure B-2: Processing options

- Use RISS email address to specify the email address for the RISS.
- Use Maximum queue size to specify the maximum number of messages that can be queued before no more messages are sent to the RISS.
- Use Options to specify the processing options to be used when Email Miner encounters an error while processing.

Select Journal to specify that the Domino journal database is to be processed.

Use File paths to specify the file path for the inherent journal databases. By default, the value is 'mailrn.nsf'.

Use Options to specify the journal processing options.

Select Delete after sending to specify that the documents within the journal be deleted after being sent to the RISS.

- Select Selective to specify that selective archiving be processed.

Use RISS Domain to specify the domain value for the RISS.

Use RISS host name to specify the URL for the RISS.

Use Tombstone message to specify the verbiage that will be present within the 'Body' of a message that has been archived.

- Use Options to specify the options for the selective archiving processing.

Select Deploy to client to create a client deployment email for each user.

Use Hotspot to specify the 'hotspot' text within the email.

Use From to specify the sender of the email.

Use Subject to specify the subject of the email.

Use Message to specify the message (instructions) for the user.

The screenshot shows the 'Options' tab of a configuration window. It contains several fields and checkboxes:

- RISS email address:** A text field with a browse button (F1).
- Maximum queue size:** A text field with a value of 0 and a browse button (F1).
- Options:** Two checkboxes, 'Journal' and 'Selective', both of which are checked.
- Journal | Selective:** A sub-tab area with 'Journal' selected.
- File paths:** A text field with a value of 'mail\m.nsf' and a browse button (F1).
- Options:** A checkbox labeled 'Delete after sending' which is checked.

Figure B-3: Message and Title fields

Use Title to specify the title of the user's confirmation dialog box that displays upon a successful deployment.

Use Message to specify the message of the user's confirmation dialog box that displays upon a successful deployment.

- Select Query RISS to require a duplication document check before sending any document to the RISS.

4. Specify the 'Logging' options

The screenshot shows the 'Logging' tab of a configuration window. It contains two fields:

- Retention:** A text field with a value of 7 and a unit of 'days'.
- Type:** A radio button group with four options: 'Summary' (selected), 'Verbose', 'Extensive', and 'Debug'.

Figure B-4: Logging options

- Use Retention to specify how many days the log documents are to be retained.
- Use Type to specify the type of logging that Email Miner should generate

Select Summary if you want Email Miner to only report basic information and errors. This will log the start and end times of the Email Miner agent, what processes are schedule to run and with what mail user Email Miner started and ended.

Select Verbose if you want Email Miner to log information per mail user processed. This will also log the start and end times for each mail database, as well as the restriction being applied to each user.

Select Extensive if you want Email Miner to log information per mail user processed. This will log more information for each mail user.

Select Debug if you want Email Miner to log extremely detailed information per mail user processed.

Note: This is recommended only for troubleshooting purposes.

5. Specify the 'Options'

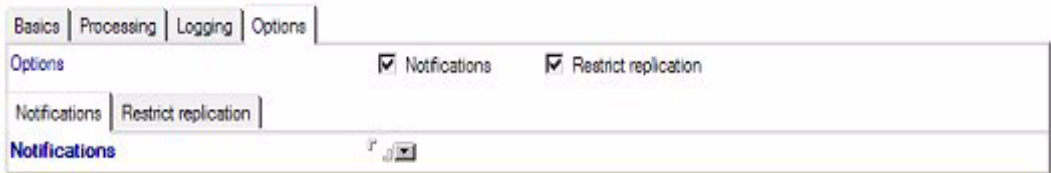


Figure B-5: Options

- Select Notifications to have Email Miner automatically notify the administrators if it encounters an error while processing.

Use Notifications to specify who should be notified.

- Select Restrict replication to prevent all server-specific information from replicating to all servers. This used to reduce the size of the Email Miner database on the servers.

Use Replication servers to specify the servers that are to contain the server-specific information for the servers within this Server Definition document.

Server status

Within Email Miner, you can view a mail server's processing history including what mail users have been processed. You may also view what information was processed and if the process is currently running.

This is done by opening view Administration\1. Servers\2. Status. This view will display a document for every mail server.

Server	Start/End Time	Process Information
Server1/ACME -- Release 5.0.9a January 7, 2002	08/27/2004 10:00:15 PM - 08/27/2004 11:38:24 PM	Processed (Debug Logging) ... -- 1,426 Mail Users

Figure B-6: Server Status

This view displays the server name, the last start/end time and what processes were executed. If opened during the execution of Email Miner, you will see the mail user currently being processed within the 'Process Information' column. The mail users are processed alphabetically (by first name/last name).

If Email Miner did not finish its execution due to any reason, Email Miner will begin with the mail user listed the next time it starts, it will begin with the mail user listed, and proceed forward until the last mail user is processed.

Specify mail user processing options

If you want to alter the Email Miner processing, perform the following steps:

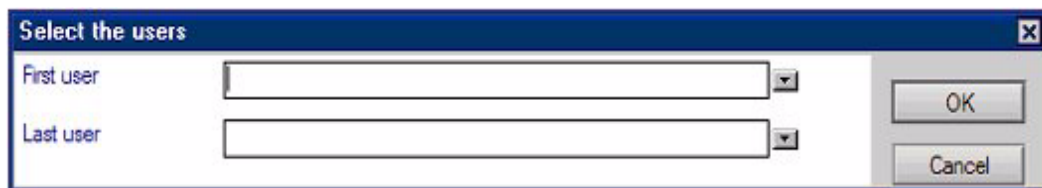
1. Select the Server Status

Select the Server Status document that you want to affect.

2. Click the button

Click  found at the top of the view.

3. Select the options



The dialog box titled "Select the users" has a blue header bar with a close button (X) in the top right corner. It contains two text input fields. The first field is labeled "First user" and has a dropdown arrow on its right side. The second field is labeled "Last user" and also has a dropdown arrow on its right side. To the right of the input fields are two buttons: "OK" and "Cancel".

Figure B-7: Specify mail user processing options

- Use First user to specify with what user the Email Miner should begin.
- Use Last user to specify with what user the Email Miner should end.

Mail user configuration

Email Miner will only manage the mail users that have a Mail User Information document within the Email Miner database. If a document does not exist for a mail user within Email Miner, the mail database will NOT be processed.

There are two ways to create Mail User Information documents within Email Miner. You can either do it manually using the Import User process, or can automate it with the Synchronize with Address Book process.

Import users

This is a manual process and gives you complete control over what mail users are processed. The import will allow you to select mail users based upon explicit name, group membership, or mail server. During the import process, the mail users being imported will display, and when complete, the total number of mail users imported will display.

To Import Users, perform the following steps:

1. Select Actions | 1. Import Users

Import'."/>

IMPORT USERS

Import information

Type ☒ By mail server ☐ By specifics

Options ☐ Include mail-in databases ☐ Use debug logging
☐ Include resource databases ☐ Use server common name

Imports

To import the users, click [Import](#)

Bold field text denotes required field

Figure B-8: Import users

- Use Type to specify how Email Miner should locate the mail users.
 Select By mail server to import the users using the home server names.

Select By specifics to import the users using specific group/user names.

Use Options to specify the import options.

Select Include mail-in databases to import mail-in database documents.

Select Include resource databases to import resource database documents.

Select Use debug logging to create additional logging information during the import process. This does not affect the import processing.

Select Use server common name to also locate the address book documents using the common name only of the servers. This is useful when the address book documents only specify the common name of the server.

- Use Imports to specify either the server or group/user names, depending on the Type selection.

2. Click Import

Click Import to start the import. Use Type to specify how Email Miner should locate the mail users.

Note: Email Miner will NOT add duplicate Mail User Information documents and will skip any mail user that is not found within the address Book. Email Miner will also skip any address book document that does not have a mail server or mail file specified.

3. Click Exit

Click Exit to close the import.

The Import document is automatically saved and can be viewed within the Administration\1. Servers\4. Imports view.

Synchronize with Address Book

This is an automated process that allows you to specify what mail users should be automatically synchronized. You can specify if you want to add, delete and/or update the Mail User Information. The Name and Address Book is used as a reference only, and will NOT be updated by this process.

Synchronize with Address Book is used to automatically synchronize the mail users within the Email Miner database with the documents within the address book. This process does NOT modify the address book.

To create and complete a Synchronize with Address Book, perform the following steps:

1. Select Create | Administration | 3. Synchronize with Address Book

hp
invent

SYNCHRONIZE WITH ADDRESS BOOK

Basic

Server	<input type="text"/>
Domain	<input type="text"/>
Actions	<input checked="" type="checkbox"/> Create <input checked="" type="checkbox"/> Delete <input checked="" type="checkbox"/> Update
Options	<input checked="" type="checkbox"/> Include mail-in databases <input checked="" type="checkbox"/> Restrict mail users <input checked="" type="checkbox"/> Include resource databases
Restrict mail users	
Restriction type	<input type="radio"/> By groups <input checked="" type="radio"/> By servers
Restriction method	<input type="radio"/> Exclude <input checked="" type="radio"/> Include
Restrictions	<input type="text"/>

Bold field text denotes required field

Figure B-9: Synchronize with Address Book

- Use Server to the server that is to process the synchronization. There should never be more than one synchronization document per server, because only one will be processed. Multiple synchronization documents are necessary when needing to synchronize multiple domains or to partially synchronize a domain.
- Use Domain to specify the name of the domain being synchronized. Email Miner will use this value to qualify the address book documents. If an address book document does not contain this value within its domain field, the document will not be processed.

- Use Actions to specify what should occur within the Mail User Information documents.

Select Create to automatically create Mail User Information documents when a new address book document has been created.

Select Delete to automatically delete Mail User Information documents when a corresponding address book document no longer exists.

Select Update to automatically update the Mail User Information documents when the corresponding address book document has changed (e.g. server, file path).

- Use Options to specify the synchronization options.

Select Include mail-in databases to synchronize the mail-in database documents within the address book.

Select Include resource databases to synchronize the resource database documents within the address book.

Restrict mail users	
Restriction type	<input type="radio"/> By groups <input checked="" type="radio"/> By servers
Restriction method	<input type="radio"/> Exclude <input checked="" type="radio"/> Include
Restrictions	F...

Figure B-10: Include resource database

Select Restrict mail users when needing to synchronize only a subset of the domain.

Use Restriction type to specify how to restrict the mail users.

Select By groups when wanting to restrict using group names.

Select By servers when wanting to restrict using server names.

Use Restriction method to specify whether to include or exclude the restricted names.

Select Exclude to synchronize all domain documents except for the ones specified.

Select Include to only synchronize the domain documents specified.

Use Restrictions to specify the mail users to be restricted.

2. Enable the Synchronization Agent

You must enable the Email Miner Synchronization agent. If the agent is not enabled, the synchronization process will not occur. Make sure that you specify the server on which the Email Miner Synchronization agent is to run. You may choose any server on which this agent is to run, but it is recommended that you specify the server where the administrators make address book changes. The Email Miner Synchronization agent should only execute on one server per domain, unless you are distributed in your administration. The Email Miner database must be present on that server.

If you need more than one synchronization process (multiple domains), copy/paste the Email Miner Synchronization agent, and change it accordingly.

The Email Miner Synchronization agent runs locally on the specified server, meaning that it does not connect to any other server while it is executing.

Note: Please allow enough time for the synchronization agent to run and the changes to replicate out to the Email Miner replicas BEFORE the Email Miner agent runs on each replica. Failure to do so could result in replication/save conflicts within the Email Miner database.

Selective archiving

Methods

Email Miner manages documents using three different methods. These methods can work in conjunction with each other, meaning that you can manage documents all three ways for the same mail user.

1. Content - The administrators can manage the documents by content. This allows the administrators to specify keywords/phrases and manage the documents that contain the specified keywords/phrases.
2. Retention - The administrator can manage the documents by retention. Within the document restriction, the administrator would specify the

maximum age for the documents, thus managing any document that is older than the maximum age.

3. Size - The administrator can manage the documents by the document size. Within the document restriction, the administrator would specify the maximum size for the documents, thus managing any document that is larger than the maximum size.

Multiple restrictions

Multiple 'Document' Mail Restrictions can exist for different folders/views with different retention periods. For example, a restriction managing the 'Inbox' can exist with a retention period of 90 days as well as a second restriction managing the 'Sent' view with a retention period of 180 days.

If two 'Document' Mail Restrictions have the same priority and different retentions for the same folder, the restriction that was last modified will take precedence.

Basics

To create and complete a Mail Restriction, perform the following steps:

1. Select Create | Administration | 2. Mail Restriction

MAIL RESTRICTION

Basics | Document | Server | User | Chronology

Status ☒ Enabled ☐ Disabled

Title

Priority ☒ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Comments

Bold field text denotes required field

Figure B-11: Creating a mail restriction

- Use Status to specify the status of the Mail Restriction.

Select Enabled to activate the Mail Restriction. This will allow the Mail Restriction to be processed by the Email Miner agent.

Select Disabled to deactivate the Mail Restriction.

- Use Title to specify a title for the Mail Restriction. This value does not affect processing.
- Use Priority to specify the priority of the Mail Restriction. This allows the administrators to create multiple mail restrictions for the same process, and Email Miner will use the Mail Restriction that has the highest priority (1 - low, 9 - high) for that process. For instance, two mail restrictions exist, the first with a priority of '1', and the second with a priority of '2'. The first one is applicable to all mail users, but the second is only applicable to a group. When Email Miner processes a mail user that belongs to the specified group, the Mail Restriction that has a priority of '2' will be used. Conversely, when Email Miner processes a mail user that does NOT belong to the specified group, the Mail Restriction that has a priority of '1' will be used. If two Mail Restrictions exist that manage the same process for the same mail user with the same priority, the Mail Restriction that was last modified will take precedence. There is an exception to this rule. If two Mail Restrictions of the same type have an identical priority for the same mail user, and one is set to NOT process the Mail Restriction and the other is set to process the Mail Restriction, the Mail Restriction that is set to NOT process the Mail Restriction will take precedence.
- Use Comments to specify any Mail Restriction specific comments that you want to make regarding the Mail Restriction. This value does not affect processing.

Document

1. Basics

Basics	Document	Server	User
Method	<input checked="" type="checkbox"/> Manage documents		
Type	<input type="radio"/> Content <input checked="" type="radio"/> Retention <input type="radio"/> Size		
Retention method	<input checked="" type="radio"/> Creation <input type="radio"/> Delivery <input type="radio"/> Modification <input type="radio"/> Posted		
Retention type	<input checked="" type="radio"/> # of Days <input type="radio"/> Date range		
Retention amount	<input type="text"/> days		
Folders	<input type="text"/>		

Figure B-12: Basics

- Use Method to specify if the documents should be managed.
- Use Type to specify how to locate the documents.
 - Select Content to locate using keywords/phrases.
 - Select Retention to locate using the document age.
 - Select Size to locate using the document size.
- Use Retention method to specify how to determine the age of the documents.
 - Use Secondary retention method to specify the secondary method to be sued in the event that the primary retention field does not exist.
- Use Retention type to specify the document retention type.
 - Select # of Days to specify a dynamic age.
 - Use Retention amount to specify the age of the documents.
 - Select Date range to specify a date range (start/end dates).
- Use Folders to specify the folders/views to be processed.

2. Method options

Specify the options specific to the method chosen for document management.

a. Content

Content

Syntax

Test syntax

Figure B-13: Content

- Use Syntax to specify the keywords/phrases to be used.
- b. Size

Size | Foldering | Options

Maximum size 10 mb

Options ☐ Include documents with attachments

Figure B-14: Size

- Use Size to specify the threshold size for the documents. Any document larger than this size will be mined.
- Use Options to specify the size options.

Select Include documents with attachments to include documents that contain attachments.

3. Folder specific options

Folder specifics

Options

☒ Exclude folders ☒ Include protect from archive

☒ Include calendar entries ☒ Include stationery

☒ Include foldered ☒ Include tasks

☒ Include non-completed tasks

Exclude folders

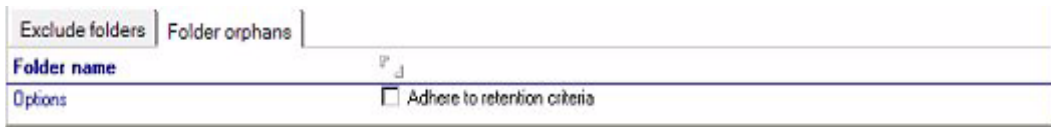
Folder names

Figure B-15: Folder specific options

- Use Options to specify the folder specifics options.

Select Exclude folders to specify that documents within special personal folders, should be excluded.

Use Folder names to specify the names of the folders. Wildcards (e.g. Protected*) can be used.



Exclude folders	Folder orphans
Folder name	
Options	
<input type="checkbox"/> Adhere to retention criteria	

Figure B-16: Exclude folders

- Select Include calendar entries to include calendar entries.
- Select Include foldered to include documents that exist in personal folders.
- Select Include protect from archive to include documents that are protected from archiving.
- Select Include stationery to include stationery documents.
- Select Include tasks to include todos.
- Select Include non-completed tasks to include tasks that have not been marked as completed.

Servers



Basics	Document	Server	User
Server specification			
<input type="radio"/> All <input checked="" type="radio"/> Exclude <input type="radio"/> Include			
Servers			

Figure B-17: Servers

- Use Server specification to specify what servers are to use the restriction.
 - Select All to specify all servers.
 - Select Exclude for all servers, except for specified servers.
 - Select Include for specified servers only.
- Use Servers to specify the servers. The administrators can enter groups (nested groups), OU structures and/or explicit server names.

Users

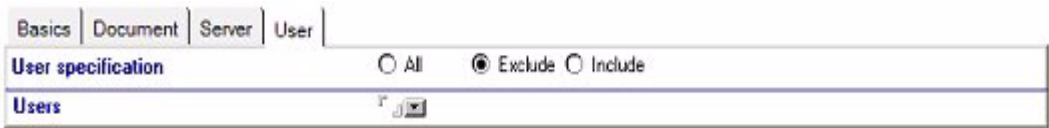


Figure B-18: Users

- Use User specification to specify what users are to use the restriction.
Select All to specify all users.
Select Exclude for all users, except for specified users.
Select Include for specified users only.
- Use Users to specify the users. The administrators can enter groups (nested groups), OU structures and/or explicit user names.

Agents

Email Miner agent

The Email Miner agent processes all of the mail restrictions as well as gathering mail database information and updating the logs. Each agent only processes the mail users that are defined to that server.

Email Miner RISS agent

The Email Miner RISS agent sends the appropriate documents from the journal and/or mail databases to the RISS.

Email Miner Tombstone agent

The Email Miner Tombstone agent creates a tombstone within the documents that have been selectively archived from the mail databases. This tombstone will designate that the document has been successfully sent to the RISS.

Error messages

Email Miner can generate numerous error messages. Each error message is categorized as either 'expected' or 'unexpected'.

An 'expected' error is caused by a configuration problem within Email Miner, the mail databases, or address Book. Email Miner generates all 'expected' errors.

An 'unexpected error' is caused when Email Miner encounters an error from LotusScript that was not expected. These errors are passed directly on to the Email Miner log.

Email Miner uses three different methods for error notifications.

- Dialog box messages
- Email notifications
- Log messages

The error messages that Email Miner generates are categorized within the appropriate message method.

If an error is reported by Email Miner and is NOT in any of the lists, please contact HP technical support.

Dialog Box messages

Different messages could appear within a dialog box while using Email Miner.

Could not open Public Name and Address Book

Email Miner was unable to open the Public Name and Address Book that is specified within the current 'Location' document.

Update the current 'Location' document to specify the proper server.

If problem persists, contact HP technical support.

The Email Miner Agent MUST execute via a schedule

This will occur if you attempt to manually execute the Email Miner scheduled agents.

Schedule the agent.

Email notifications

Email Miner could generate emails when a severe problem occurs. The error is placed into the subject of the email. The emails are automatically sent to whoever has 'Manager' rights to the Email Miner database.

A Server Definition does not exist for 'Server'. Email Miner will not execute until a Server Definition is created.

Email Miner could not locate a Server Definition document for the 'server' specified.

Either create a Server Definition document for the server, or include the server in an existing Server Definition document.

If problem persists, contact HP technical support.

Log messages

Email Miner could generate various messages that are placed within the log documents. Each log document that contains one of these errors will be marked with an exclamation point. The following table lists the log messages.

Table B-1: Email Miner Log Messages

Log message number	Log message	Cause	Action
ERR0001	Could not find Server Definition for 'xxx'	The Server Definition for the specified server ('xxx') cannot be found within Email Miner.	Contact HP technical support.
ERR0011	Could not find view 'Mail Restrictions'	The 'Mail Restrictions' view cannot be found within the Email Miner database.	Contact HP technical support.
ERR0012	Could not find view 'Deployments'	The 'Deployments' view cannot be found within the Email Miner database.	Contact HP technical support.
ERR0013	Could not find view 'Mail Users Information By Server'	The 'Mail Users Information By Server' view cannot be found within the Email Miner database.	Contact HP technical support.
ERR0014	Could not find view 'Server Definitions'	The 'Server Definitions' view cannot be found within the Email Miner database.	Contact HP technical support.
ERR0015	Could not find view 'Server Statuses'	The 'Server Statuses' view cannot be found within the Email Miner database.	Contact HP technical support.
ERR0016	Could not open Public Name and Address Book	The address book is not available to be used.	Contact HP technical support.

Table B-1: Email Miner Log Messages (continued)

Log message number	Log message	Cause	Action
ERR0017	Could not find view '(\$VIMGroups)' in Public Name and Address Book	The '(\$VIMGroups)' view cannot be found within the address book.	Contact HP technical support.
ERR0018	Could not open Reference database	The reference database is not available to be used.	Contact HP technical support.
ERR0019	Insufficient access for Reference database	The agent signer does not have the proper access to the Email Miner Reference database.	Grant the agent signer at least "Editor" access within the ACL of the Email Miner Reference database.
ERR0020	Could not find view 'Reference UNIDs'	The 'Reference UNIDs' view cannot be found within the Email Miner Reference database.	Contact HP technical support.
ERR0021	'xxx' could not access mail database for 'yyy' (zzz)	The agent signer (where xxx is the agent signer) could not access the mail database (where zzz is the file path) for a user (where yyy is the user name).	Alter the ACL of the mail database.
ERR0022	Only have 'xxx' access to mail database for 'yyy'	The agent signer does not have sufficient access (where xxx is the access) to the mail database (where yyy is the user name).	Alter the ACL of the mail database.

Table B-1: Email Miner Log Messages (continued)

Log message number	Log message	Cause	Action
ERR0023	Could not find mail database for 'xxx' (yyy)	The mail database for a user (where xxx is the user name and yyy is the file path) could not be located.	Ensure that the mail database has not been moved/deleted.
ERR0024	Stopped processing due to request by 'xxx' at yyy	The agent stopped processing due to a request by xxx (where xxx is the administrator name) at yyy (where yyy is the time of the stop request).	No action required.
ERR0025	Stopped processing due to maximum agent execution time of xxx minutes	The agent stopped because it exceeded the maximum execution time (where xxx is the maximum number of minutes).	No action required.
ERR0026	'xxx' could not set quota for 'yyy' (zzz). Check 'Server' document (within Public Name and Address Book) for 'Administrators' value.	The agent signer does not have administrator rights for the servers.	Update the administrators value in the server document.

Table B-1: Email Miner Log Messages (continued)

Log message number	Log message	Cause	Action
ERR0027	Stopped processing folder 'xxx' (Error encountered)	A 'Bad document ID/key' error occurred while processing a folder during 'Content' processing.	Contact HP technical support.
ERR0028	Could not find view '(\$VIMPeople)' in Public Name and Address Book	The '(\$VIMPeople)' view cannot be found within the address book.	Contact HP technical support.
ERR0029	Could not find view 'Mail Users Information By Name'	The 'Mail Users Information By Name' view cannot be found within the Email Miner database.	Contact HP technical support.

INDEX

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

- access control lists. See ACLs
- Account Manager window, PAM [3-4](#), [3-8](#)
- accounts, user [3-2](#)
- acknowledging problems
 - host [2-129](#), [2-144](#)
 - service [2-136](#), [2-144](#)
- ACLs
 - adding [3-25](#)
 - adding to repositories [3-22](#)
 - filtering list of [3-24](#)
 - removing from repositories [3-22](#)
 - removing users [3-25](#)
 - user profiles [3-26](#)
 - users, adding or removing [3-25](#)
 - viewing information [3-21](#), [3-24](#)
- active smart cell group, definition [2-48](#)
- address book, Email Miner [B-11](#)
- Agent view [2-118](#)
- agents, Email Miner [B-19](#)
- Alert Histogram view [2-94](#)
- Alert History view [2-97](#)
- Alert Summary view [2-100](#)
- All Warnings view [2-120](#)
- Application Management view [2-25](#)
- applications, RIM [1-3](#)
- archive directory, log [2-69](#), [2-92](#)

- Archive Request file [4-3](#), [4-16](#)
- Archive Request Loader [4-6](#)
- archiving of data, definition [1-2](#)
- ASSIGNED smart cell state,
 - definition [2-13](#)
- Availability view [2-85](#)

B

- BACKING_UP smart cell state,
 - definition [2-13](#)
- backup library, definition [2-47](#)
- backup system [2-46](#)

C

- catchall repository
 - definition [2-77](#)
 - PAM [3-34](#)
- cloning a smart cell [2-36](#)
- CLOSED smart cell state, definition [2-13](#)
- collection objects, PAM
 - adding members to [3-12](#)
 - definition [3-9](#)
 - removing members [3-13](#)

- commands, PCC
 - external [2-143](#)
 - host [2-128](#)
 - hostgroup [2-123](#)
 - overriding [2-143](#)
 - process [2-69](#)
 - service [2-133](#), [2-135](#)
 - View Config view [2-112](#)
- comments
 - host [2-131](#), [2-144](#)
 - service [2-133](#), [2-139](#)
 - user [3-18](#)
 - view [2-63](#)
- COMPLETE_PROCESSING smart cell
 - state, definition [2-13](#)
- conditions, status
 - definition [2-12](#)
 - hard and soft [2-15](#)
- contacts [2-110](#)
- CRITICAL service status value,
 - definition [2-15](#)

D

- DAS
 - configuring [2-28](#)
 - displaying configuration
 - associations [2-33](#)
 - displaying servers [2-35](#)
 - starting or scheduling jobs [2-34](#)
- data archiving, definition [1-2](#)
- Data Backup panel [2-48](#)
- data querying, definition [1-2](#)
- DEAD smart cell state, definition [2-14](#)
- directories, log and log
 - archive [2-69](#), [2-92](#)
- disabling notifications [2-144](#)
- DISCOVERY smart cell state,
 - definition [2-13](#)
- Document Manager
 - description [1-3](#)

- domain smart cells [2-20](#)
- domain-affiliated smart cells [2-115](#)
- Domino server configuration [5-14](#)
- DOWN host status value, definition [2-14](#)
- downtime, scheduling
 - host groups [2-123](#)
 - hosts [2-130](#)
 - queue view [2-73](#)
 - rescheduling services [2-74](#)
 - services [2-137](#)
 - viewing [2-65](#)
- duplicate signature backup
 - services [2-46](#), [2-47](#)
- Dynamic Account Synchronization
 - See DAS

E

- editing reports [2-81](#)
- email
 - example of adding a new
 - department [3-39](#)
 - Microsoft Exchange [5-2](#)
 - routing filters [3-34](#)
 - text summary reports [2-79](#)
 - user information, modifying [3-17](#)
- Email Miner
 - about [A-2](#)
 - address book, synchronizing [B-11](#)
 - administration guide [B-1](#)
 - agents [B-19](#)
 - archiving [B-13](#)
 - description [1-4](#)
 - Document options [B-15](#)
 - error messages [A-12](#), [B-20](#)
 - frequently asked questions [A-2](#)
 - importing users [B-9](#)
 - installing [A-7](#)
 - mail server configuration [B-3](#)
 - processing options [B-8](#)
 - restrictions [B-14](#)

- security [B-2](#)
- Server Definition [B-3](#)
- Server options [B-18](#)
- Server Status [B-7](#)
- upgrading [A-4](#), [A-10](#)
- user configuration [B-9](#)
- User options [B-19](#)
- enabling notifications [2-144](#)
- error messages
 - Email Miner administration [B-20](#)
 - Email Miner installation [A-12](#)
- event log
 - Alert History view [2-97](#)
 - Notifications view [2-89](#)
 - rotation [2-69](#), [2-92](#)
- Exchange server [2-42](#)
- Exchange, Microsoft
 - journal mining [5-3](#)
 - mailbox mining [5-5](#)
 - non-sticky ports [5-7](#)
 - publishing forms [5-6](#)
 - stub support [5-6](#)
 - user accounts [5-2](#)
- External Command Interface view [2-143](#)

F

- FileSpec tag, PST Importer [4-18](#)
- filtering lists
 - ACLs [3-24](#)
 - repositories [3-20](#)
 - routing filters [3-37](#)
 - routing rules [3-28](#)
 - simple routing rules [3-32](#)
 - users [3-16](#)
- filters, routing [3-34](#)
- flap detection [2-139](#)
- FREE smart cell state, definition [2-13](#)

G

- graphs, System Status view [2-21](#)
- groups, smart cells [2-23](#)

H

- HARD status condition, definition [2-15](#)
- Header tags, PST Importer [4-16](#)
- health, checking system [2-18](#)
- Help menu, PAM [3-5](#)
- history
 - alerts [2-97](#)
 - patches [2-106](#)
- Host Commands section [2-128](#)
- Host Detail view [2-56](#)
- host groups
 - All Warnings view [2-120](#)
 - Availability view [2-85](#)
 - definition [2-11](#)
 - downtime, scheduling [2-123](#)
 - Information view [2-121](#)
 - notifications [2-124](#)
 - service checks [2-125](#)
 - Service Overview view [2-58](#)
 - software version, viewing [2-106](#)
 - Status Grid view [2-141](#)
 - status, displaying [2-18](#)
 - View Cell Space view [2-113](#)
 - View Config view [2-108](#)
- Host Information view [2-126](#)
- Host Problems view [2-62](#)
- Host Status Totals [2-17](#), [2-18](#), [2-56](#)
- Host/Service commands box, PCC [2-144](#)
- Hostgroup Commands [2-123](#)
- Hostgroup Information view [2-121](#)

hosts

- Availability view [2-85](#)
- commands [2-128](#)
- comments, adding [2-131](#)
- downtimes, scheduling [2-130](#)
- Host Detail view [2-56](#)
- Host Information view [2-126](#)
- notifications [2-129](#), [2-130](#)
- problems, viewing [2-62](#)
- service checks [2-131](#)
- Service Detail view [2-53](#)
- Service Overview view [2-58](#)
- software version, viewing [2-106](#)
- Status Grid view [2-141](#)
- status, displaying [2-18](#)
- Tactical Monitoring view [2-51](#)
- Trends view [2-81](#)
- View Cell Space view [2-113](#)
- View Config view [2-107](#)
- HP StorageWorks Reference Information
 - Storage System, definition [1-2](#)
- HTTP Portals, View Cell Space
 - view [2-113](#)
- HTTP servers, starting, stopping, or restarting [2-25](#)

I

- importing users, Email Miner [B-9](#)
- installing
 - Email Miner [A-7](#)
 - Lotus Notes plug-in [5-15](#)
 - Outlook plug-in [5-8](#)
 - PAM [3-2](#)
 - PST Importer [4-4](#)

J

- JBoss components
 - Agent view [2-118](#)
 - MBean view [2-117](#)
- Job Assignments [2-34](#)
- journal mining [5-3](#)

L

- LDAP servers
 - configuring DAS [2-28](#)
 - deleting connections [2-33](#)
- left menu, PCC
 - definition [2-3](#)
 - views [2-8](#)
- library, backup, definition [2-47](#)
- life cycle states
 - definition [2-12](#)
 - types of [2-13](#)
- logging in to PAM [3-3](#)
- logs
 - notifications [2-89](#)
 - PST Importer [4-14](#), [4-15](#)
 - rotation [2-69](#), [2-92](#)
- lost smart cell pseudostate [2-20](#), [2-113](#)
- Lotus Notes
 - Email Miner administration guide [B-1](#)
 - Email Miner installation guide [A-2](#)
 - plug-in, installing [5-15](#)
 - system configuration [5-14](#)

M

- Mail Attender for Exchange
 - description [1-4](#)
- mailbox mining [5-5](#)
- mappings, updating or deleting [2-33](#)

MBean components
 Agent view [2-118](#)
 MBean view [2-117](#)
MBean view [2-117](#)
menus, PAM [3-4](#)
MetaServer, View Cell Space view [2-113](#)
Microsoft Exchange
 journal mining [5-3](#)
 mailbox mining [5-5](#)
 non-sticky ports [5-7](#)
 publishing forms [5-6](#)
 stub support [5-6](#)
 user accounts [5-2](#)
Microsoft Outlook plug-in, installing [5-8](#)
Mining Overview view [2-42](#)
monitoring, PCC [2-11](#), [2-50](#)

N

Nagios Info view [2-68](#)
Nagios Stats view [2-71](#)
non-sticky ports, configuring [5-7](#)
notifications
 Alert Histogram view [2-94](#)
 Alert History view [2-97](#)
 Alert Summary view [2-100](#)
 detailed email reports [2-77](#)
 disabling during downtime [2-65](#)
 disabling for all hosts and
 services [2-69](#)
 editing reports [2-81](#)
 enabling and disabling [2-144](#)
 host groups [2-124](#)
 host, enabling or disabling [2-129](#)
 hosts [2-130](#)
 service [2-136](#)
 text-summary reports [2-79](#)
 viewing [2-89](#)
Notifications view [2-89](#)

O

objects, PAM
 adding members to collections [3-12](#)
 creating [3-8](#)
 deleting [3-11](#)
 modifying [3-10](#)
 removing members from
 collections [3-13](#)
 viewing [3-8](#)
OK service status value, definition [2-15](#)
Options menu, PAM [3-5](#)
Outlook plug-in, installing [5-8](#)

P

PAM
 about [3-1](#)
 Account Manager window [3-4](#), [3-8](#)
 ACLs panel [3-23](#)
 adding ACLs [3-25](#)
 adding ACLs to repositories [3-22](#)
 adding repositories [3-21](#)
 adding routing filters [3-37](#)
 adding routing rules [3-29](#)
 adding simple routing rules [3-33](#)
 adding users [3-17](#)
 Catchall Repository [3-34](#)
 collection objects, adding members
 to [3-12](#)
 comments, user [3-18](#)
 creating objects [3-8](#)
 definition [3-2](#)
 deleting objects [3-11](#)
 deleting routing filters [3-38](#)
 deleting routing rules [3-30](#)
 description [1-3](#)
 email information, modifying [3-17](#)
 example of adding a new
 department [3-39](#)
 filtering users list [3-16](#)
 installing [3-2](#)

logging in [3-3](#)
menus [3-4](#)
modifying objects [3-10](#)
modifying routing filters [3-38](#)
modifying routing rules [3-30](#)
profiles, user [3-26](#)
removing ACLs from repositories [3-22](#)
removing collection object
 members [3-13](#)
Repositories tab [3-9](#)
repositories, creating, modifying,
 deleting [3-19](#)
Routing Filters panel [3-34](#)
Routing Rules panel [3-27](#)
Simple Routing Rules panel [3-31](#)
user accounts [3-2](#)
Users panel [3-14](#)
users, adding to ACLs [3-25](#)
users, removing from ACLs [3-25](#)
viewing ACL information [3-24](#)
viewing objects [3-8](#)
viewing repository information [3-21](#)
viewing routing rules [3-28](#)
viewing user information [3-16](#)
patches [2-106](#)
PCC
 about [2-1](#)
 accessing [2-3](#)
 acknowledging
 problems [2-129](#), [2-136](#), [2-144](#)
 administration tasks [2-6](#)
 Agent view [2-118](#)
 Alert Histogram view [2-94](#)
 Alert History view [2-97](#)
 Alert Summary view [2-100](#)
 All Warnings view [2-120](#)
 Application Management view [2-25](#)
 Availability view [2-85](#)
 backup [2-46](#)
 commands [2-123](#), [2-133](#), [2-135](#), [2-143](#)
 commands, overriding [2-143](#)
 Comments view [2-63](#)
 comments, host [2-131](#), [2-144](#)
 comments, service [2-139](#)
 contacts [2-110](#)
 description [1-3](#)
 detailed email reports [2-77](#)
 downtime, host groups [2-123](#)
 downtime, hosts [2-130](#)
 downtime, scheduling [2-65](#)
 downtime, services [2-137](#)
 editing reports [2-81](#)
 External Command Interface
 view [2-143](#)
 flap detection [2-139](#)
 groups, smart cells [2-23](#)
 health, checking system [2-18](#)
 host commands [2-128](#)
 Host Detail view [2-56](#)
 Host/Service commands box [2-144](#)
 Hostgroup Information view [2-121](#)
 left menu [2-3](#), [2-8](#)
 MBean view [2-117](#)
 Mining overview view [2-42](#)
 monitoring [2-50](#)
 monitoring tools [2-11](#)
 Nagios Info view [2-68](#)
 Nagios Stats view [2-71](#)
 notifications for host groups [2-124](#)
 notifications for hosts [2-129](#)
 notifications for services [2-130](#)
 Notifications view [2-89](#)
 notifications, enabling and
 disabling [2-144](#)
 patch history [2-106](#)
 polling [2-12](#)
 printing [2-7](#)
 process commands [2-69](#)
 Process Commands box [2-69](#)
 Process State Information chart [2-69](#)
 Program Information chart [2-68](#)
 refreshing views [2-7](#)
 Replication view [2-39](#)
 rescheduling services [2-74](#)

- Scheduling Queue view [2-73](#)
- service checks [2-125](#), [2-131](#), [2-138](#)
- Service Detail view [2-53](#)
- Service Information view [2-133](#)
- service notifications [2-136](#)
- Service Overview view [2-58](#)
- Service Problems view [2-61](#)
- smart cell life cycle states [2-13](#)
- states [2-12](#)
- status conditions [2-12](#)
- Status Grid view [2-141](#)
- Status Summary view [2-17](#)
- System Backup view [2-46](#)
- System Status view [2-20](#)
- Tactical Monitoring view [2-50](#)
- text-summary reports [2-79](#)
- Tivoli Console [2-49](#)
- Trends view [2-81](#)
- updating views [2-7](#)
- user interface [2-4](#)
- User Management view [2-28](#)
- View Cell Space view [2-113](#)
- View Config view [2-107](#)
- views [2-3](#), [2-4](#), [2-6](#)
- PENDING status value, definition [2-14](#)
- Platform Account Manager. See PAM
- Platform Control Center. See PCC
- polling of hosts and services [2-12](#)
- primary signature backup
 - services [2-46](#), [2-47](#)
- primary smart cells [2-115](#)
- printing PCC views [2-7](#)
- problems view [2-61](#)
- Process Commands box [2-69](#)
- Process State Information chart, Nagios
 - Info view [2-69](#)
- Program Information chart, Nagios Info
 - view [2-68](#)
- PST Import Monitor [4-11](#)
- PST Importer
 - about [4-1](#)
 - Archive Request File [4-3](#)

- Archive Request file [4-16](#)
- Archive Request Loader [4-6](#)
 - description [1-4](#)
 - features [4-2](#)
- FileSpec tag [4-18](#)
- Header tags [4-16](#)
- installing [4-4](#)
- logs [4-14](#), [4-15](#)
- process [4-2](#)
- PST Import Monitor [4-11](#)
- sample file [4-19](#)
- Status Monitor report [4-15](#)

Q

- querying, definition [1-2](#)

R

- R00000000 Catchall Repository [3-34](#)
- registry keys
 - Microsoft Exchange [5-4](#)
 - Outlook plug-in [5-8](#)
- Replication view [2-39](#)
- replication, smart cells used for [2-115](#)
- reports
 - Alert Histogram view [2-94](#)
 - Alert History view [2-97](#)
 - Alert Summary view [2-100](#)
 - availability [2-88](#)
 - detailed [2-77](#)
 - editing [2-81](#)
 - PST Importer [4-14](#)
 - text-summary [2-79](#)
 - Trends view [2-81](#)
- repositories
 - adding [3-21](#)
 - adding ACLs [3-22](#)
 - catchall, definition [2-77](#)
 - catchall, PAM [3-34](#)

- creating, modifying, deleting [3-19](#)
- definition [3-2](#)
- filtering list of [3-20](#)
- removing ACLs [3-22](#)
- routing rules [3-30](#)
- simple routing rules [3-33](#)
- viewing information [3-21](#)
- Repositories tab, PAM [3-9](#)
- Repository ID [3-34](#)
- requirements
 - Email Miner [A-5](#)
 - PST Importer [4-4](#)
- rescheduling services [2-74](#)
- RESET smart cell state, definition [2-13](#)
- restarting servers [2-25](#)
- RESTORE smart cell state,
 - definition [2-14](#)
- restoring data on failed smart cells [2-116](#)
- retention file [2-108](#), [2-110](#)
- RIM, application programs for users [1-3](#)
- RISS
 - applications [1-3](#)
- RISS Lotus Notes Interface
 - description [1-3](#)
- RISS Outlook Interface
 - description [1-3](#)
- RISS Web Interface
 - description [1-3](#)
- rotation, event log file [2-69](#), [2-92](#)
- routing filters
 - adding [3-37](#)
 - Catchall Repository [3-34](#)
 - definition [3-34](#)
 - deleting [3-38](#)
 - examples [3-35](#)
 - modifying [3-38](#)
 - panel [3-34](#)
- Routing Filters panel [3-34](#)
- routing rules
 - adding [3-29](#)
 - adding simple [3-33](#)
 - deleting [3-30](#)

- filtering list of [3-28](#)
- modifying [3-30](#)
- panel [3-27](#)
- repositories [3-30](#)
- simple [3-31](#)
- viewing information [3-28](#)
- Routing Rules panel [3-27](#)

S

- scenarios, adding a new
 - department [3-39](#)
- scheduling downtime
 - host groups [2-123](#)
 - hosts [2-130](#)
 - rescheduling services [2-74](#)
 - services [2-137](#)
 - viewing [2-65](#)
- Scheduling Queue view [2-73](#)
- secondary smart cells [2-115](#)
- security, Email Miner [B-2](#)
- selective archiving [2-42](#)
- Server Definition, Email Miner [B-3](#)
- servers
 - DAS, configuring [2-28](#)
 - DAS, displaying [2-35](#)
 - Domino, configuring [5-14](#)
 - Email Miner [B-3](#)
 - Exchange [2-42](#)
 - LDAP [2-33](#)
 - mailbox mining [5-5](#)
 - mappings, updating or deleting [2-33](#)
 - mining [2-42](#)
 - starting, stopping, or restarting [2-25](#)
- service checks
 - host groups [2-125](#)
 - hosts [2-131](#)
 - services [2-138](#)
- Service Commands section [2-135](#)
- Service Detail view [2-53](#)
- Service Information view [2-133](#)

- Service Overview view, PCC [2-58](#)
- Service Problems view [2-61](#)
- Service Status Totals [2-17](#), [2-18](#), [2-56](#)
- services
 - commands [2-133](#), [2-135](#)
 - comments [2-139](#)
 - Status Grid view [2-141](#)
 - Trends view [2-81](#)
 - View Config view [2-109](#)
- signature backup, definition [2-46](#)
- Signatures panel [2-47](#)
- Simple Routing Rules panel [3-31](#)
- smart cells
 - active groups [2-48](#)
 - cloning [2-36](#)
 - domain [2-20](#)
 - domain-affiliated [2-115](#)
 - groups [2-23](#)
 - lost [2-20](#), [2-113](#)
 - MBeans [2-119](#)
 - primary [2-115](#)
 - replication, used for [2-115](#)
 - restoring data on [2-116](#)
 - secondary [2-115](#)
 - state, life cycles [2-12](#)
 - states, life cycle
 - types of [2-13](#)
 - System Status view [2-20](#)
 - unaffiliated [2-114](#), [2-115](#)
- SMTP Portals, View Cell Space
 - view [2-113](#)
- SMTP Servers, starting, stopping, or restarting [2-25](#)
- SOFT status condition, definition [2-15](#)
- software versions [2-20](#), [2-23](#), [2-106](#)
- states
 - definition [2-12](#)
 - types of [2-13](#)
- status conditions
 - definition [2-12](#)
 - hard and soft [2-15](#)
- Status Grid view [2-141](#)

- Status Monitor report, PST
 - Importer [4-15](#)
- Status Summary view, PCC [2-17](#)
- status values
 - definition [2-12](#)
 - normal [2-14](#)
- stub support, configuring [5-6](#)
- stub, definition [4-2](#)
- SUSPENDED smart cell state,
 - definition [2-14](#)
- SYNC_WAIT smart cell state,
 - definition [2-13](#)
- synchronizing address book, Email Miner [B-11](#)
- System Backup view [2-46](#)
- system requirements
 - Email Miner [A-5](#)
 - PST Importer [4-4](#)
- System Status view [2-20](#)

T

- Tactical Monitoring view [2-50](#)
- time periods, View Config view [2-111](#)
- Tivoli Console [2-49](#)
- Tivoli web site [2-48](#)
- Tombstone agent, Email Miner [B-19](#)
- tombstone, definition [4-2](#)
- Trends view [2-81](#)
- troubleshooting
 - Email Miner administration [B-20](#)
 - Email Miner installation [A-12](#)
- TSC-NAT, View Cell Space view [2-113](#)

U

- unaffiliated smart cells [2-114](#), [2-115](#)
- UNKNOWN service status value,
 - definition [2-15](#)

UNREACHABLE host status value,
 definition [2-15](#)
UP host status value, definition [2-14](#)
upgrading Email Miner [A-4](#), [A-10](#)
User Management view [2-28](#)
users
 accounts [3-2](#)
 adding new [3-17](#)
 adding to ACLs [3-25](#)
 comments, modifying [3-18](#)
 email information, modifying [3-17](#)
 Email Miner [B-9](#)
 filtering list of [3-16](#)
 Microsoft Exchange [5-2](#)
 Outlook plug-in [5-12](#)
 PCC management [2-28](#)
 profiles [3-26](#)
 removing from ACLs [3-25](#)
 Users panel [3-14](#)
 viewing information [3-16](#)
Users panel [3-14](#)

V

value, status
 definition [2-12](#)
 normal values [2-14](#)
version identifier,
 viewing [2-20](#), [2-23](#), [2-106](#)
View Cell Space view [2-113](#)
View Config view [2-107](#)
View menu, PAM [3-5](#)
view, PCC, definition [2-3](#)

W

WARNING service status value,
 definition [2-15](#)
WORM media, backup to [2-46](#)